Applicant Details

First Name	**Sarah**
Last Name	**Al-Shalash**
Citizenship Status	**U. S. Citizen**
Email Address	**sa3992@columbia.edu**
Address	**Address** Street **419 W 119th Street, 8C1** City **New York** State/Territory **New York** Zip **10027** Country **United States**
Contact Phone Number	**2144712150**
Other Phone Number	**2144712150**

Applicant Education

BA/BS From	**Yale University**
Date of BA/BS	**May 2019**
JD/LLB From	**Columbia University School of Law** **http://www.law.columbia.edu**
Date of JD/LLB	**May 15, 2024**
Class Rank	**School does not rank**
Law Review/Journal	**Yes**
Journal(s)	**Science and Technology Law Review**
Moot Court Experience	**No**

Bar Admission

Prior Judicial Experience

Judicial Internships/Externships	**No**

Post-graduate Judicial Law Clerk	**No**

Specialized Work Experience

Recommenders

Emens, Elizabeth
eemens@law.columbia.edu
212-854-8879

Greene, Jamal
jamal.greene@law.columbia.edu
212-854-5865

Richman, Dan
drichm@law.columbia.edu
212-854-9370

This applicant has certified that all data entered in this profile and any application documents are true and correct.

Sarah Al-Shalash
419 W 119th Street, 8C1
New York, NY 10027
214-471-2150

June 11, 2023

The Honorable Kenneth M. Karas
United States District Court
Southern District of New York
Charles L. Brieant, Jr. United States Courthouse
300 Quarropas Street, Room 533
White Plains, NY 10601-4150

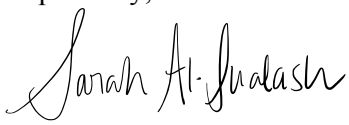
Dear Judge Karas:

I am a rising third-year student, a James Kent Scholar, and a Public Interest/Public Service Fellow at Columbia Law School. I am also the Executive Articles Editor of the *Science and Technology Law Review*. I write to apply for a clerkship in your chambers beginning in 2024, or for any term thereafter. As a student committed to a career in service of the public interest, I hope to use my clerkship to become a more effective advocate for the communities I serve. I believe the experience I will gain and mentorship I will receive in your chambers will allow me to do just that. I am particularly interested in clerking in your chambers because of your commitment to a collegial environment and a culture of mentorship, two values you embodied when you came to speak to Columbia's Clerkship Diversity Initiative.

Furthermore, I believe I would be an excellent clerk. I have long enjoyed legal research and writing, and I've honed that enjoyment into a skill as a legal research assistant, a litigation intern at the American Civil Liberties Union, and a member of the *Science and Technology Law Review*. I take pride in being a warm and collaborative colleague, a trait that I found universally useful in my professional life prior to law school. I am disciplined, attentive, and ever-curious. I hope to bring these qualities to bear in my work in your chambers.

Enclosed please find a resume, transcript, and writing sample. Also enclosed are letters of recommendation from Professor Jamal Greene (jamal.greene@law.columbia.edu), Elizabeth Emens (eemens@law.columbia.edu), and Daniel Richman (drichm@law.columbia.edu). Thank you for your time and continued consideration of my candidacy.

Respectfully,



Sarah Al-Shalash

SARAH AL-SHALASH

419 West 119th Street, Apt. 8C1, New York, NY 10027
214-471-2150 • sarah.al-shalash@columbia.edu

EDUCATION

COLUMBIA LAW SCHOOL, New York, NY
J.D., expected May 2024
Honors: Public Interest/Public Sector Fellow, James Kent Scholar, Harlan Fiske Stone Scholar
Activities: Columbia Science and Technology Law Review (Executive Articles Editor), CLS Legal Tech Association (Public Interest Events Chair), Academic Coach, Research Assistant to Professor Elizabeth Emens, Research Assistant to Professor Jamal Greene, Teaching Assistant to Professor Thomas Merrill, Human Rights Institute 1L Advocates Program.

YALE UNIVERSITY, New Haven, CT
B.A., in Ethics, Politics, and Economics, received May 2019
Honors: Class of 2019 Commencement Marshall
Activities: The Yale Politic Magazine; Fifth Humour Sketch Comedy group; Worked approximately 20 hours per week to finance education

EXPERIENCE

American Civil Liberties Union — New York, NY
Speech, Privacy, and Technology Team Internship — May 2023 – August 2023

Knight First Amendment Institute — New York, NY
Litigation Extern — August 2022 – December 2022
Research Assistant, Press Freedom Project — January 2022 – April 2022
Supported innovative litigation efforts about issues related to digital rights and the First Amendment, such as: the use of spyware by powerful officials, Texas and Florida laws targeting social media sites, and surveillance of journalists.

Electronic Privacy Information Center (EPIC) — Washington, DC
Internet Public Interest Opportunities Program Clerkship — May 2022 – August 2022
Performed tasks focused on privacy in the digital age. Drafted legal memoranda regarding Federal Trade Commission (FTC) complaints, wrote model amicus brief about Section 230 immunity, drafted Freedom of Information Act (FOIA) request regarding surveillance of individuals in prisons, supported legislative efforts regarding the American Data Privacy and Protection Act (ADDPA).

Deloitte Government & Public Service — Washington, DC
Consultant — October 2019 – August 2021
Supported a number of projects at the intersection of technology and the public interest. Completed internal projects with Deloitte's Trustworthy and Ethical Technology team and Deloitte's 5G team.

LANGUAGES: Arabic (heritage speaker); French (fluent)

Columbia
Law School

Registration Services

law.columbia.edu/registration
435 West 116th Street, Box A-25
New York, NY 10027
T 212 854 2668
registrar@law.columbia.edu

CLS TRANSCRIPT (Unofficial)

06/08/2023 16:59:29

Program: Juris Doctor

Sarah Al-Shalash

Spring 2023

Course ID	Course Name	Instructor(s)	Points	Final Grade
L6407-1	Advanced Constitutional Law: 1st Amendment	Healy, Thomas Joseph	3.0	A
L6905-1	Antidiscrimination Law	Johnson, Olatunde C.A.	3.0	B+
L6472-1	S. Special Topics in Federal Courts	Schmidt, Thomas P.	2.0	A
L6683-1	Supervised Research Paper	Richman, Daniel	2.0	A
L6822-1	Teaching Fellows	Merrill, Thomas W.	4.0	CR

Total Registered Points: 14.0

Total Earned Points: 14.0

Fall 2022

Course ID	Course Name	Instructor(s)	Points	Final Grade
L6241-2	Evidence	Capra, Daniel	4.0	A
L6299-1	Ex. The Knight First Amendment Institute	DeCell, Caroline; Diakun, Anna	2.0	A
L6299-2	Ex. The Knight First Amendment Institute - Fieldwork	DeCell, Caroline; Diakun, Anna	3.0	CR
L6425-1	Federal Courts	Metzger, Gillian	4.0	A-
L6675-1	Major Writing Credit	Richman, Daniel	0.0	CR
L6685-1	Serv-Unpaid Faculty Research Assistant	Emens, Elizabeth F.	2.0	A
L6683-1	Supervised Research Paper	Richman, Daniel	1.0	A

Total Registered Points: 16.0

Total Earned Points: 16.0

Spring 2022

Course ID	Course Name	Instructor(s)	Points	Final Grade
L6108-4	Criminal Law	Seo, Sarah A.	3.0	B+
L6679-1	Foundation Year Moot Court		0.0	CR
L6474-1	Law of the Political Process	Greene, Jamal	3.0	A-
L6121-11	Legal Practice Workshop II	Harwood, Christopher B	1.0	P
L6116-4	Property	Merrill, Thomas W.	4.0	A-
L6118-2	Torts	Rapaczynski, Andrzej	4.0	A

Total Registered Points: 15.0

Total Earned Points: 15.0

January 2022

Course ID	Course Name	Instructor(s)	Points	Final Grade
L6130-7	Legal Methods II: Contemporary Issues in Constitutional Law	Liu, Goodwin	1.0	CR

Total Registered Points: 1.0

Total Earned Points: 1.0

Fall 2021

Course ID	Course Name	Instructor(s)	Points	Final Grade
L6101-2	Civil Procedure	Genty, Philip M.	4.0	B+
L6133-1	Constitutional Law	Greene, Jamal	4.0	B+
L6105-4	Contracts	Emens, Elizabeth F.	4.0	A-
L6113-2	Legal Methods	Briffault, Richard	1.0	CR
L6115-11	Legal Practice Workshop I	Harwood, Christopher B; Hong, Eunice	2.0	P

Total Registered Points: 15.0

Total Earned Points: 15.0

Total Registered JD Program Points: 61.0

Total Earned JD Program Points: 61.0

Honors and Prizes

Academic Year	Honor / Prize	Award Class
2022-23	James Kent Scholar	2L
2021-22	Harlan Fiske Stone	1L

June 11, 2023

The Honorable Kenneth Karas
Charles L. Brieant, Jr. United States Courthouse
300 Quarropas Street, Room 533
White Plains, NY 10601-4150

Dear Judge Karas:

I am writing to recommend Ms. Sarah Al-Shalash for a clerkship in your chambers. Ms. Al-Shalash is a very smart, engaging, and thoughtful law student, who I expect will be a terrific clerk.

I know Ms. Al-Shalash in two ways: as a student in my Contracts class in Fall 2021 and as my Research Assistant during the Summer through Fall of 2022. I therefore have a strong basis on which to comment on her performance and prospects.

My introduction to Ms. Al-Shalash came through first-year Contracts in the Fall of 2021. The grades in that course were based primarily on a difficult anonymously graded exam, which combined multiple-choice questions and essays. Students were required to write two essays: one analyzing traditional legal problems in order to predict how a court would decide them, and a second evaluating the conceptual underpinnings of contract law and applying them to specific doctrines. The exam also required students to apply their knowledge of doctrine to solve problems on a set of challenging multiple-choice questions. Ms. Al-Shalash did a fine job on all three portions of the exam, and she earned an "A-" in the course. She was also a thoughtful class participant, memorably so.

Based on her terrific performance in Contracts, I invited Ms. Al-Shalash to become my Research Assistant (RA) beginning in the Summer of 2022. My RAs submit written memos to me, and they also present their findings to each other and to me in periodic RA Briefing Meetings. Ms. Al-Shalash conducted interdisciplinary research on widely varying topics related generally to gender and disability discrimination. She wrote strong memos on these topics and presented her work effectively in the Briefing Meetings. She earned an "A" in this position.

Ms. Al-Shalash has had an impressive law-school career so far, both inside and outside the classroom. She earned Harlan Fiske Stone Honors for her academic performance during her 1L year, and, because of her demonstrated commitment to pursuing a career in civil/human rights law and technology, she is a Public Interest/Public Service Fellow at the Law School. She is currently Executive Articles Editor for the *Columbia Science and Technology Review*, overseeing a team of nearly forty Articles Editors and Staff Editors and serving as the key liaison between the journal and the authors. She has served as the Public Interest Event Planning Chair for the Columbia Legal Technology Association; a CLS Peer Mentor; a Clerkship Diversity Initiative Scholar; and a member of the 1L Human Rights Advocates Program. Many of these activities involve mentoring others, which is a lifelong passion of hers.

She has sought out research and teaching opportunities during her first two years at Columbia, externing with the Knight First Amendment Institute, which is an appellate litigation public interest organization focused on protecting civil liberties in the digital age, and serving as a Research Assistant to Professor Jamal Greene as well as to me. She has served as a Teaching Assistant for Property and as an Academic Coach for several students in the subject of Contract Law.

During her summers, Ms. Al-Shalash has been gaining experience that builds on her already strong skill set. She spent her 1L summer at the Electronic Privacy Information Center, where she worked on amicus briefs regarding Section 230 liability and supported advocacy efforts for federal privacy legislation. Currently, Ms. Al-Shalash is working at the ACLU Speech, Privacy and Technology Project.

Before law school, Ms. Al-Shalash worked for two years as a Consultant in Deloitte's Public Sector practice. In this role, she served a variety of public sector clients, including the Department of Defense and Nadia's Initiative (a non-profit begun by Nobel Peace Prize Winner Nadia Murad). This role required her to work in a fast-paced environment, to collaborate with across teams and with clients, to adjust to new settings quickly, and to be extremely attentive to detail. Ms. Al-Shalash's interest in the law long predates that job, however; at sixteen, she was listening to Supreme Court oral arguments in her spare time.

On a personal note, I might add two points. First, her commitment to public service work comes from her experience growing up in an Iraqi family, a Muslim girl in a conservative Texas town. Second, before law school, Ms. Al-Shalash was a comedic performer; this was her main extracurricular activity in high school and college. This taught her about taking risks and integrating others' responses into her performance, which has helped her become someone who takes feedback in stride.

In sum, Ms. Al-Shalash is a smart, talented, and engaging law student deeply committed to public service. I believe she will be a terrific clerk, and I strongly recommend her to you.

Let me know if I can provide any other information. I would be happy to speak further. I am out of the office this Summer, but recommendations are a priority, and I can generally be reached through my assistant, Kiana Taghavi (ktaghavi@law.columbia.edu), or on my cell phone at 718-578-9469.

Sincerely,

Elizabeth Emens - eemens@law.columbia.edu - 212-854-8879

Elizabeth F. Emens

Elizabeth Emens - eemens@law.columbia.edu - 212-854-8879

June 11, 2023

The Honorable Kenneth Karas
Charles L. Brieant, Jr. United States Courthouse
300 Quarropas Street, Room 533
White Plains, NY 10601-4150

Dear Judge Karas:

I write in support of Sarah Al-Shalash's application to clerk in your chambers. Having gotten to know Sarah as her professor for two classes and in her capacity as my research assistant, I would cheerfully hire her myself if I were a judge. I hope to persuade you to hold her in similarly high esteem.

To put first things first, Sarah is an excellent law student. It shows in her grades, but they understate her legal ability. I first came to know Sarah in her first semester of law school, when she was a student in my 33-student Constitutional Law "small group." The "small group" experience allows a professor to become well acquainted with the class—everyone in the class was on call many times over the course of the semester, class participation was encouraged even for students who were not on call, and office hours were lively, often continuing topics raised in class with most of the class members present. I find a class of this size especially valuable for Constitutional Law, a course whose subject matter can expose students to vulnerabilities that are easier for them to experience—and for the professor to manage—in a more intimate setting. Sarah excelled in this environment. She was always well-prepared, was deeply curious, and was respectful of others. She was also remarkably self-possessed, exuding an intellectual maturity that one does not always encounter in first-year law students. I genuinely looked forward to her interventions, which I came over the course of the semester to recognize as the product of a preternaturally thoughtful mind.

The downside of a small group is that the class size typically produces an unusual number of excellent exams, which makes the grading curve especially unforgiving of strong performers who miss a random point here or there on the final. Sarah produced the 11th highest exam score, but this was good for just a B+: only the top 10 scores could receive A-level grades. Her exam was a strong one by any reasonable measure.

In her second semester of law school, Sarah enrolled in my 126-student Law of the Political Process class. Law of the Political Process is a theoretically rigorous election law class that immerses students in the constitutional and statutory doctrine around voting rights, rights of political association, districting and gerrymandering, and campaign finance. The course was extremely demanding. It required advanced competence in constitutional law, comfort with interpretation of several complex statutes, an ability to navigate confusing and self-contradictory case law with Byzantine factual records, and the agility to move back and forth between the highly conceptual and the highly specific. Students reported the workload as unusually heavy for a three-credit course. The course attracts highly motivated students, many of whom have already done related advanced coursework and a surprising number of whom have previous professional experiences in election-related settings. For these reasons, the course has in the past been limited to upperclass students —the year Sarah took the course was the first time 1L students were permitted to enroll. Despite being a 1L, Sarah was again a high performer, submitting a top-25 exam out of the 126 students in the course.

Impressed by her legal acumen, her maturity, and her demeanor, I asked Sarah if she might be interested in serving as a research assistant for me in the fall of 2022 to provide support for an ongoing book project. She agreed, and I gave her two of the more difficult assignments I have given any RA in recent years. The first project required her to research the empirical relationship between women's access to reproductive care in the 1960s and 1970s and their levels of civic participation; the second required her to scour the legislative record to see the how members of Congress defended the constitutionality of the Civil Rights Act of 1875 over the several years in which aspects of the law were being debated. For the latter project, Sarah was almost entirely self-directed, structured her own time and organization of the research, and produced a 92-page research memo that will supply material crucial to the book project. I had high expectations for what Sarah would produce as a research assistant, and she far exceeded them.

Purely in terms of the work of a judicial clerk—the legal analysis, the bench memos, the draft opinions and orders, the reliability and maturity—Sarah is a high-upside, low-risk candidate. But those are not the only reasons to give her your highest consideration. Sarah also would bring to chambers a diverse set of life experiences, acquired at significant personal cost to her. Sarah was born in Texas to two Iraqi immigrants. After a three-year move to Versailles, where her father pursued work as an engineer, Sarah's family returned to Texas, where she spent most of her childhood. What might have been an idyllic middle-class life in the Dallas suburbs for some was a whirlwind of Islamophobia, racism and xenophobia for a Muslim family that had spent three years living in France. Sarah overcame insults and hostility to become a star student and debater before heading to Yale for college. There she experienced another culture shock, this time based in class, and again had to overcome cultural alienation—leaving home, which women in her community rarely did before marriage, had strained her relationship with her family.

It would be understandable for someone to become withdrawn and embittered by these experiences, but Sarah has drawn strength from adversity. She embraces challenges—whether it's the Great Books course at Yale or Law of the Political Process at Columbia—she is a voracious consumer of legal writing, and she has genuine personal and professional commitments, in her case to decoupling the relationship between technology and power. She's also a delightful—and very funny—person (she was a comedic performer from age 14 to 22, and directed a sketch comedy group in college). As I said, if I were a judge, Sarah would be a top choice. She should be one for you too.

Jamal Greene - jamal.greene@law.columbia.edu - 212-854-5865

Thank you for your kind consideration. Please do not hesitate to reach out if I can be of additional assistance.

Sincerely,

Jamal Greene
Dwight Professor of Law

COLUMBIA LAW SCHOOL
435 West 116th Street
New York, NY 10027

June 11, 2023

The Honorable Kenneth Karas
Charles L. Brieant, Jr. United States Courthouse
300 Quarropas Street, Room 533
White Plains, NY 10601-4150

Re: Sarah Al-Shalash

Dear Judge Karas:

I write to enthusiastically support the application of Sarah Al-Shalash – a rising 3L at Columbia Law School, Class of 2024 -- to be your law clerk. She is whip smart, writes beautifully, and would doubtlessly do extraordinary work in your chambers. She's also a delightful and inspiring person.

I first met Sarah during her 1L year, when I was assigned to be her mentor as part of the Public Interest/Public Service Fellows Program. She had been selected for that program, in part, because of her undergraduate work at Yale, and the work she did before law school for Deloitte – as a public sector consultant working with, among other clients, Space Force(!) – and at the State Department. As she has explained to me:

When I began my undergrad career, I was interested in international relations.
Specifically, I was interested in the Middle East, and the role of the West in Middle Eastern conflict. I thought I would work for a non-profit or in an aid organization.

In pursuit of this goal, I applied for an internship at the State Department. I wanted to
work for an embassy in the Middle East. Unfortunately, I was waitlisted for the positions I was most interested in. Instead, I was offered a position at one of the bureaus in DC. This bureau was relatively new, and very modern. They were working on issues of technology in international relations. My internship was the summer of 2017, and the 2016 election loomed large then. Most of my work focused on disinformation and misinformation, and I fell in love with the issues at the edge of this new horizon.

Sarah has gone to work with organizations grappling with the hardest digital privacy issues – EPIC, the Knight Institute, and (this summer) the ACLU. And she used her 2L Note for the Science and Technology Law Review for just such an issue, under my supervision. She chose quite a challenging topic: does the Fourth Amendment restrict reverse keyword searches by the Government, and, if not, what other doctrinal resources might be available. The topic was challenging for several reasons. To begin, just finding judicial discussions of the issue was hard. Although there is good evidence that law enforcement agencies are using subpoenas (not warrants) to obtain this information, judicial analyses are sparse. Sarah rose to that challenge by looking to not just the limited cases precisely on point but to the growing number of cases involving geofence warrants – another reverse search, whose analysis offers some analogies. But the real challenge for Sarah, given her commitments to privacy protections, was facing up to the limits of the Fourth Amendment in the area, and recognizing that even current First Amendment doctrine would offer little help. Sarah rose to this challenge as well, never letting her ideological preferences get in the way of cold case law analysis and always aware of the limits of constitutional protection.

Sarah was an utter pleasure to work with. She can write quickly and powerfully, and is deft indeed at case law analysis. Moreover, it was a pleasure to work with her, as she responds to criticism speedily and effectively.

Sarah's grades are quite good, particularly after her first semester 1L year. I often find that students who have not gone directly from college don't immediately take to law school exams. But she now seems to be firing on all cylinders.

Only when I pushed Sarah for her personal backstory did I realize the extent of her personal accomplishment and strength of character. She grew up in Plano, Texas, the daughter of Iraqi immigrants (her dad escaped Iraq on foot to avoid conscription into the Iraqi army during the 1990 Gulf War). Her time in the Dallas area was often painful:

I watched my teachers and classmates cheer on the war in Iraq as my mother fielded phone calls from back home, telling her that her family members had been brutally murdered on the streets of Baghdad. Everyone around me seemed to accept that my culture and my religion was something to be feared and denounced. My entire childhood, I experienced strong Islamophobia and anti-Arab prejudice.

The experience led her to work hard, in hopes of going to college outside of Texas. But her acceptance to Yale led to only more difficulties, as her parents refused to let her leave home, and ended up cutting her off financially. Attending Yale without the money to buy required books was a life-changing experience:

For better or for worse, that experience taught me a lot. It taught me how to be gritty, and how to work hard even when it feels like the odds are stacked against you. I took a full course load, worked 2-3 student jobs per semester, and ran several student organizations. In the summer, I always took one "resume" job (an internship that would be relevant to my career), and 3-4 "real"

jobs (jobs that I knew would give me the reserves for another year of school). Eventually, this all became second nature to me, and the struggles I felt so acutely in my first few years of school began to feel manageable.

Against this backdrop, Sarah's law school performance and the professional path she has charted are indeed a triumph.

I think you'd like Sarah a lot and am confident she'd be a spectacular law clerk. Her commitment to public interest work, top-notch intellect, and proven record of sustained and excellent writing would enrich any Chamber. Both in print and in person, she expresses herself clearly and with tight analytical lines. She's also a lovely person – calm, mature, with a wonderful sense of humor (she ran a sketch comedy group at Yale) and real leadership skills (she was a Yale Commencement Marshal). You'll love working with her and watching her soar thereafter when she continues her public interest work. If there is anything else I can add, please give me a call.

Respectfully yours,

Daniel Richman

Dan Richman - drichm@law.columbia.edu - 212-854-9370

SARAH AL-SHALASH
Columbia Law School J.D. '24
214-417-2150
sarah.al-shalash@columbia.edu

CLERKSHIP APPLICATION WRITING SAMPLE

The writing sample below is an excerpt from my student Note: *Finding A Needle In A Haystack: Reverse Keyword Searches, Speech, And Privacy*. The Note discusses the advent of reverse keyword searches, a novel investigative method by which law enforcement can compel Google and other online search providers to divulge the information of any and all users who searched for a particular set of terms; if they believe these searches will reveal the perpetrator of or witnesses to a particular crime. The Note makes two claims: First, that existing Fourth Amendment doctrine does not protect against these forms of search, and that this lack of protection should be cause for concern. Second, that the First Amendment can and should provide a buttress against law enforcement uses of reverse keyword searches.

The excerpt below touches on the first point: that the Fourth Amendment is likely to be insufficiently protective of the civil liberties interests implicated by these investigative methods. Only one case thus far has litigated the constitutionality of reverse keyword searches. Therefore, in order to predict the constitutional analysis that will be applied to future challenges to reverse keyword searches, I rely heavily on another, similar form of search—the geofence search. A geofence search is a similar law enforcement investigative tool which allows police to compel companies like Google to turn over the information of individuals who were recorded as being in or near a particular place during the time at which a crime occurred.

This Note benefited from substantive feedback from my Note Advisor, Professor Daniel Richman.

PART II: APPLYING THE FOURTH AMENDMENT TO REVERSE SEARCH WARRANTS

a. Introduction

Very little litigation about reverse keyword searches has been undertaken.[1] This part of the Note attempts to fill this gap in the literature by assessing the current state of Fourth Amendment doctrine, particularly with respect to reverse searches, and using that information to determine how courts might apply that doctrine to reverse keyword search warrants. Because of the dearth of reverse keyword search cases, this analysis will rely heavily on the existing case law regarding geofence warrants, the reverse keyword search warrant's closest analog.

Like reverse keyword searches, geofence warrants allow law enforcement to commandeer the databases of big technology companies like Google. With one warrant, law enforcement can access millions of data points—and potential suspects. Like reverse keyword searches, geofence warrants are undertaken in order to identify a suspect, rather than with a suspect in mind. Like reverse keyword searches, the information obtained in geofence warrants is "voluntarily" given to Google when individuals use the technology company's services and implicitly or explicitly "agree" to collection of their information.[2]

---

[1] *People v. Seymour* is the only publicly available challenge to information obtained through a reverse keyword search warrant. Motion to Suppress Evidence from a Keyword Warrant & Request for a Veracity Hearing at ¶ 2, *People v. Seymour*, No. 21CR20001 (Colo. 2022) ("No court has considered the legality of a reverse keyword search").

[2] Whether this data-sharing can be accurately described as "voluntarily given" is heavily contested, and a question that this Note attempts to grapple with. See Part II.C.ii, *infra*. Many observers of the modern data-economy argue that even where individuals know their information is being collected and stored, and even where they affirmatively accept such practices, they are nonetheless not providing "meaningful consent." *See, e.g.,* Neil Richards, Woodrow Hartzog*, Privacy's Trust Gap: A Review Obfuscation: A User's Guide for Privacy and Protest by Finn Brunton and Helen Nissenbaum Cambridge and London: The Mit Press, 2015,* 126 YALE L.J. 1180 (2017) ("Thinking of privacy as an issue of personal choice, preferences, and responsibility has powerful appeal.[…] Yet there is a problem with this view of the digital world…[t]he digital consumer is not like the classic American myth of the cowboy, a rugged and resilient island of autonomy set against the backdrop of the digital frontier.[…] In the digital world, we may heap responsibility on individual users of technology, but they lack options for protecting themselves.").

This section will cover (i) how warrant requirements and third-party doctrine have been applied to geofence warrants, (ii) what key differences might nonetheless make the geofence analysis inapplicable to reverse keyword searches, (iii) how reverse keyword search warrants might be analyzed under existing Fourth Amendment doctrine, and (iv) how the good faith exception may apply in the context of reverse keyword search warrants. Ultimately, the analysis suggests that the Fourth Amendment is an insufficiently protective or certain guardrail on government intrusions of this nature.

b. Geofence Warrants and the Fourth Amendment

In total, geofence warrants have been challenged a total of eleven times in the lower federal courts, to mixed results—although on balance most applications have either been granted or upheld under the good faith exception.[3] On these eleven challenges, three decisions have denied the legality of the warrant, five have upheld the legality of these warrants, and three have upheld the use of the evidence from the warrant under the good faith exception.[4] This inconsistency in the lower courts is evidence of the deep uncertainty that current Fourth Amendment doctrine has

[3] The legality of geofence warrants is at issue in eleven publicly reported federal cases: *Matter of Search of Info. Stored at Premises Controlled by Google, as further described in Attachment A*, No. 20 M 297, 2020 WL 5491763 (N.D. Ill. 2020) (geofence warrant application denied); *Matter of Search of Info. Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730 (N.D. Ill. 2020) (geofence warrant application denied); *Matter of Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation*, 497 F. Supp. 3d 345 (N.D. Ill. 2020) (geofence application granted); *Matter of Search of Info. that is Stored at Premises Controlled by Google, LLC*, 542 F. Supp. 3d 1153 (D. Kan. 2021) (geofence application denied); *Matter of Search of Info. that is Stored at Premises Controlled by Google LLC*, 579 F. Supp. 3d 62 (D.D.C. 2021) (geofence warrant application granted); *United States v. Chatrie*, 590 F. Supp. 3d 901 (E.D. Va. 2022) (finding the geofence warrant was improperly issued but upholding the use of evidence under the good faith exception); United States v. Davis, 2022 WL 3007744 (M.D. Ala. July 28, 2022) (upholding the legality of the geofence warrant); *United States v. Cruz, Jr.*, No. 22-cr-0064 (D.D.C. 2023) (evidence from geofence warrant upheld because it was properly issued, else the good faith exception applied); *U.S. v. Rhine*, No. CR 21-0687 (RC), 2023 WL 372044 (D.D.C. 2023) (denying motion to suppress evidence obtained by a geofence warrant); *United States v. Smith*, No. 3:21-CR-107-SA, 2023 WL 1930747 (N.D. Miss. 2023) (finding law enforcement failed to comply with the narrowing requirement of the warrant, but upholding evidence on basis of the good faith exception); *Matter of Search of Info. Stored at Premises Controlled by Google*, 2023 WL 2236493 (S.D. Tex. 2023) (upholding the legality of the geofence warrant).

[4] *Id*.

engendered, an uncertainty driven in no small part by the rapidly changing technological landscape.[5]

State courts are another important site of contestation for geofence warrants. Here too, the evidence (such that it exists) about the court's response is mixed. In the six cases that were publicly available, state courts upheld the use of geofence warrants in three of them.[6] In one of these cases, the court found that the geofence warrant had been improperly issued, but that it was subject to the good faith exception.[7] In the remaining three cases, state courts rejected the use of geofence warrants.[8] In one of those cases, the court found that the geofence warrant had been improperly issued, that the good faith exception applied, but that notwithstanding the good faith exception the warrant was required to be excluded under California statutory law.[9]

As this catalog of publicly-available geofence cases reveals, existing doctrine about the legality of these investigative tools is best described as uncertain. Nevertheless, geofence warrants are an important analog to the reverse keyword search warrant case.

---

[5] For more on the uncertainty regarding the scope of the Fourth Amendment engendered by recent decisions like *Carpenter v. US*, see: Matthew Tokson, *The Aftermath of Carpenter: An Empirical Study of Fourth Amendment Law*, 2018-2021, 135 Harv. L. Rev. 1790, 1800 n. 64 and 65 (2022).

[6] An EFF investigation suggests that a California lower court denied a suppression motion in the *People v. Meza*. Jennifer Lynch, *EFF Files Amicus Briefs in Two Important Geofence Search Warrant Cases*, EFF (Jan. 31, 2023) (https://tinyurl.com/2s3eb5kv); In re: Motion to Suppress Geofence Evidence, *Arizona v. Batain*, 2022 Az. Superior Court (Pima County, 2022) (upholding geofence on the basis of the good faith exception) (https://tinyurl.com/2p8er85a). Reporting indicates that a geofence was permitted by a Jefferson Circuit Judge in Louisville, Kentucky for in a murder investigation of the death of Tyree Smith. Jacob Ryan, *To Solve Murders, Louisville Police Turn to Techy 'Geofence' Warrants—But Net Few Arrests*, LEO WEEKLY (Oct. 22, 2021) (https://tinyurl.com/2s4bkkrw).

[7] In re: Motion to Suppress Geofence Evidence, *Arizona v. Batain*, 2022 Az. Superior Court (Pima County, 2022).

[8] *See In re Info. Stored at the Premises Controlled by Google*, 2022 Va. Cir. (Fairfax Co. Feb. 24, 2022) (finding that a proposed geofence warrant was impermissible under the federal constitution because it was lacked particularity and probable cause); Order Granting Motion to Suppress, *People v. Dawes*, No. 19002022 (CA Super. Ct. San Francisco 2022) (finding the geofence warrant prohibited, regardless of its constitutionality, because of CalEPCA, a California statute); Memorandum of Decision and Order on Defendant's Motion to Suppress Search Warrant, *Commonwealth v. Fleischmann*, 2021 Ma. Sup. (https://tinyurl.com/59zcxwa2).

[9] Order Granting Motion to Suppress, *People v. Dawes*, No. 19002022 (CA Super. Ct. San Francisco 2022).

i. Geofence Warrants and the Third-Party Doctrine

Courts, and Google, have largely treated geofence warrants as covered by the Fourth Amendment, suggesting that they believe that *Carpenter* applies to this form of search.[10] This development may suggest that reverse keyword searches will also fall under the Fourth Amendment's protections. But there is reason to remain concerned about the Fourth Amendment's scope in this area: Courts have generally "presumed, without deciding" that *Carpenter* covers geofence warrants.[11] This language suggests that the uncertainty of *Carpenter* has been weakly papered-over by the courts, rather than resolved decisively in favor of finding reverse searches to be Fourth Amendment searches.

ii. Geofence Warrants and the Probable Cause Requirement

In the context of geofence searches, the probable cause requirement has proven flimsy. In these cases, the courts have required that (1) there is a fair probability that a crime has been committed, and (2) a fair probability that the evidence of a crime will be in the particular place to be searched (typically Google's databases).[12] Generally, the first prong of the test is easily met:

---

[10] Google maintains that geofence searches require a warrant under the SCA and the Fourth Amendment, and lower federal courts have presumed without deciding that the Fourth Amendment applies to geofence warrants. *See* Brief of Amicus Curiae Google LLC in Support of Neither Party Concerning Defendant's Motion to Suppress Evidence from a "Geofence" General Warrant, *US v. Chatrie*, 590 F.Supp.3d 901 (E.D. Va. 2022) (Arguing that it is "[C]lear that a geofence request constitutes a 'search' within the meaning of the Fourth Amendment and that, absent an applicable exception, the Constitution independently requires the government to obtain a warrant to obtain LH information. Users have a reasonable expectation of privacy in their LH information, which the government can use to retrospectively reconstruct a person's movements in granular detail. Under Carpenter, the 'third-party doctrine' does not defeat that reasonable expectation of privacy merely because users choose to store and process the information on Google' servers."). *See also, e.g.,* 590 F. Supp. 3d at 925 ("Because the Court will independently deny Chatrie's motion to suppress by considering the validity of the Geofence Warrant, the Court 'need not wade into the murky waters of standing,' i.e., whether Chatrie has a reasonable expectation of privacy in the data sought by the warrant."); 579 F. Supp. 3d 62, 74 (D.D.C. 2021) ("Because the government applied for a search warrant, the Court assumes (but does not decide) that the Fourth Amendment's restrictions on searches and seizures apply to the collection of cell phone location history information via a geofence.").

[11] *See* quotes from *US v. Chatrie* and *Matter of Search of Info. that is Stored at Premises Controlled by Google LLC supra* at note 88.

[12] 579 F. Supp. 3d at 75 (D.D.C. 2021).

law enforcement asks for a geofence warrant when it is investigating a crime for which it has no leads.[13] One might expect the second requirement to present more of a barrier, but it often does not. Courts often assume that evidence will be available on the targeted database.[14] They assume that most people carry cellphones with them, and that those cellphones (and the apps they contain) are tracking the location information of the person in question.[15]

This version of the probable cause requirement offers no meaningful constraints on government authority. In this context, it becomes a mere formality: it is fair to assume that nearly everyone has a cellphone, and it is also fair to assume that nearly everyone with a cellphone is having their location tracked by Google, Yahoo, Microsoft, Snapchat, and any number of other companies.[16]

iii. Geofence Warrants and the Particularity Requirement

---

[13] *See, e.g., id.* at 77. This may undermine some of the concerns evinced by reproductive rights activists in the wake of *Dobbs v. Jackson Women's Health Organization*, because it suggests that conducting a search to gather evidence of criminal activity (there, abortion) without evidence that a crime has occurred will likely face heightened challenges as to the probable cause requirement.

[14] *See, e.g.,* 497 F.Supp.3d at 356 ("Unlike virtually any other item, it is rare to search an individual in the modern age during the commission of a crime and not find a cell phone on the person. Thus, it is reasonable to infer that suspects coordinating multiple arsons across the city in the middle of the night, as well as any passersby witnesses, would have cell phones.").

[15] *See* 579 F.Supp.3d at 78. *In the Matter of Search of Info. that is Stored at Premises Controlled by Google LLC* (hereinafter "D.D.C case"), the court upheld the use of a geofence warrant to identify suspects alleged to have committed federal crimes in a remote, industrial location. Using the governing standard, the court determined that the requirement for probable cause had been met. The perpetrators were seen on CCTV using cellphones, and given the vastness of Google's location data troves, there was a fair probability that their information was available through a search of the company's data.

But as the court in the D.D.C. case notes, a showing that the suspect had a cellphone at the crime scene is not a requirement for finding probable cause. The court in the case says: "The core inquiry here is probability, not certainty, and it is eminently reasonable to assume that criminals, like the rest of society, possess and use cell phones to go about their daily business." The court notes that in another case, *Matter of Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation*, the district court granted a geofence warrant without evidence that the suspects possessed cellphones.

[16] 579 F.Supp.3d at 78 (noting that it would be the "relatively rare" case when a cell phone does not transmit location information to Google, noting that three-quarters of the world's phones contain Google's operating systems.).

Courts have used several factors to determine whether a geofence warrant meets the "particularity" required to issue a warrant. Typically, these factors include: geographic scope, density of the searched area, time span covered by the search, and time of search itself.[17] Ultimately, the particularity inquiry turns on how many people are reasonably likely to be caught up in a search.

Where the aforementioned factors suggest that a geofence search is likely to catch the activity of a large number of people, courts have often rejected the warrant for lack of particularity. For example, in *United States v. Chatrie*, the government had sought and obtained data from a geofence spanning over three football fields and encompassing both a bank and a church.[18] In deeming the warrant unconstitutional, the court highlighted its concern with the warrant's lack of particularity.[19] The court admonished that it was "difficult to overstate the breadth of the warrant."[20] In other cases where courts have upheld geofence warrants, they have noted the warrant's limited geographic and temporal scope, and the fact that the area covered by the warrant is unlikely to be densely populated.[21]

c. Geofence Warrant Analysis Might Not Apply Neatly to Reverse Keyword Search Warrants

Though geofence searches are, in many ways, the clearest analog to reverse keyword search warrants, the two forms of search are distinct in material ways. As to the third-party doctrine,

---

[17] *See, e.g.,* 579 F.Supp.3d at 81-2 (analyzing the temporal and geographic scope of the geofence warrant to determine whether it was appropriate); 590 F. Supp. 3d at 918 (analyzing the temporal and geographic scope of the geofence warrant to determine whether it was appropriate).

[18] 590 F. Supp. 3d at 918.

[19] *Id*. at 930.

[20] *Id.*

[21] *See, e.g.,* 579 F.Supp.3d at 81-2 (finding that three hours of location data from a six-month time span was reasonable and particular within the meaning of the Fourth Amendment, and that a geofence covering only an undisclosed location and its parking lot was sufficiently narrow to meet the particularity requirement).

reverse keyword search warrants raise fewer concerns about location information and arguably entail more affirmative consent than geofence warrants, two factors that may make the third-party doctrine more likely to apply. As to the particularity requirement, it is more difficult to assess the scope of the warrant *ex ante* in the reverse keyword search warrant context than the geofence context. Finally, as to the probable cause requirement, it may be more difficult to assume that the information being sought is in the databases of a particular search engine provide in the reverse search context.

i. Location Information Not Implicated in the Same Way by Reverse Keyword Search Warrants

Even if the Fourth Amendment does constrain geofence searches, there is reason to think that *Carpenter*, and thus the Fourth Amendment, may nonetheless be inapplicable to reverse keyword search warrants. First, because geofence warrants implicate location-information, which the court has treated as meriting special concern in the Fourth Amendment context.[22] In *Carpenter* itself, the court noted the particular protections it had extended to surveillance implicating location information.[23]

Geofences are unlike reverse keyword searches in that they reveal an individual's precise location at a certain time. At worst, reverse keyword searches may reveal where an individual *intended* to go,[24] but they do not typically reveal their precise location and movements. This distinction may be material: revealing one's *intent* to go somewhere may not trench as closely on

[22] *Carpenter v. United States*,138 S. Ct. 2206, 2215 (2018) ("The Court has in fact already shown special solicitude for location information in the third-party context").
[23] *Id.*
[24] For example, in the Colorado case, *People v. Seymour*, the reverse keyword search warrant revealed the addresses that those caught in the warrant had searched for. The prosecution contended this was evidence that the defendants *did* go to this location. *People v. Seymour*, No. 21CR20001 (2022) (https://tinyurl.com/y46t9wsb).

protected privacy interests as revealing where someone actually *was*. Furthermore, many reverse keyword search warrants do not even reveal this much; in fact, several do not implicate location at all.[25] Rather, those warrants only reveal a person's interest in a particular topic or a particular individual.

ii. Reverse Keyword Search Warrants May Entail More Affirmative Consent than Location History

Reverse keyword searches are arguably distinct from both CSLI and geofence location information in that (1) online users more affirmatively "opt-in" to collection when they *enter* that information into a particular online search with an awareness that (2) that information is being closely monitored by Google.

First, online search can be characterized as materially distinct from the location tracking at issue in *Carpenter* and in geofence searches. Unlike location tracking, which is often enabled without any affirmative action by the user,[26] online search requires a user to actively go to a website (normally Google.com), and type in their query. And this affirmative action is often taken with complete knowledge of the fact that users' search activities are being closely monitored by the company.[27] *Carpenter* establishes that sometimes, revealing information to a third party does not undermine a user's reasonable expectation of privacy in that information, particularly when

---

[25] See Section I.a.ii, *supra*, discussing the Edina case, which only requested the information of those who had looked for a victim's name.

[26] Google officially claims that it only tracks the location of users who affirmatively opt-in to tracking. *Manage Your Location History*, Google (https://tinyurl.com/4jvrt6r9). Nevertheless, recent lawsuits and investigations have suggested that this location information is still being tracked and stored, even when users believe they have opted out. Taylor Hatmaker, *Google Gets Hit With a New Lawsuit Over 'Deceptive' Location Tracking*, TECH CRUNCH, Jan. 24, 2022 (https://tinyurl.com/6j7zr9md). Cecilia Kiang, *Google Agrees to $392 Million Privacy Settlement With 40 States*, N.Y. Times, Nov. 14, 2022 (https://tinyurl.com/6j7zr9md).

[27] Emilee Rader, *Awareness of Behavioral Tracking and Information Privacy Concern in Facebook and Google*, 14 SOUPS 51, 58-60 (study suggests that many internet users expect that Google is collecting what they are typing into the search bar, regardless of whether they actually submit the information).

information collection is subtle and the user has limited alternative options.[28] But in the case of online search, research suggests that the information collection in question is widely known, and there are alternative options (but query whether these alternatives are legitimate).[29] These distinctions suggest that at the very least, reverse keyword searches may be less likely to fall within the *Carpenter* doctrine than geofence warrants, their closest analog.

Second, geofence searches arguably come closer to the automatic CLSI collection in *Carpenter* than reverse keyword searches.[30] Traditional third-party doctrine assumes that an individual gives up their right to privacy by consensually revealing information to the third-party.[31] *Carpenter* found that the CSLI, though in a sense "voluntarily" handed over to cellphone companies, nevertheless could not truly be considered consensual because individuals had little meaningful choice in revealing that information.[32]

Like the CSLI in *Carpenter*, location information is often collected by companies like Google without much meaningful consent from users.[33] Like the CSLI in *Carpenter*, companies like Google track location information by default on users' phones. And echoing the argument

---

[28] *See supra* note 73.

[29] Companies like DuckDuckGo actively market their search engines as more private, less-invasive alternatives to Google search. *Privacy*, DUCKDUCKGO, https://tinyurl.com/2p87fsxn. For more alternatives, see: *Matt Burgess, Four Privacy-First Google Search Alternatives You Need to Try*, WIRED (Aug. 30, 2021), https://tinyurl.com/mwkt88vh. Arguably, this suggests that users of Google Search have "assumed the risk" of having their search queries collected and disseminated to law enforcement under the logic of *Miller* and *Smith*.

[30] Google has argued that location information is, in fact, *more* invasive than CSLI. Brief of Amicus Curiae Google LLC in Support of Neither Party Concerning Defendant's Motion to Suppress Evidence from a "Geofence" General Warrant, *US v. Chatrie*, 590 F.Supp.3d 901 (E.D. Va. 2022) ("Moreover, LH information can often reveal a user's location and movements with a much higher degree of precision than CSLI and other types of data. And rather than targeting the electronic communications of only a specific user or users of interest, the steps Google must take to respond to a geofence request entail the government's broad and intrusive search across Google users' LH information to determine which users' devices may have been present in the area of interest within the requested timeframe.")

[31] *See supra* note 66, and accompanying text.

[32] 138 S. Ct. at 2220 (Arguing that CSLI is unlike traditional forms of third-party data because individuals are constantly compelled to use cellphones, and by the very fact of using those cellphones, sending location information to cell towers. The Court argues that without an "affirmative" act, there cannot be "meaningful" voluntary consent).

[33] *See supra* note 104.

made and accepted in *Carpenter*, individuals can hardly "opt-out" of having a cellphone in the modern world.[34] While users can opt out of location collection, Google makes it incredibly difficult for them to do so, and sometimes even covertly continues collection.[35] Thus, unlike the CSLI in *Carpenter*, the collection of location information is not a condition of owning a cellphone, but given the difficulty of intervening in such collection, it is arguably similarly non-consensual.

iii. More Difficult to Understand the Scope of Reverse Keyword Search Warrants *Ex Ante*

Geofences that extend over a large or densely-populated area, or that span a long period of time, are sometimes subject to scrutiny related to the particularity requirement.[36] It's difficult to see how similar limiting standards will be imposed on reverse keyword search warrants *a priori*. Under the particularity requirement, courts make a determination about the reasonableness of the scope of a search before the warrant is issued. Thus, in the case of reverse keyword searches, courts are obliged to guess, at the outset, how many individuals' information will be captured in the reverse search. This is true in the case of geofence warrants as well, but the criteria that the courts look to to make that determination (geographic scope, length of time, density of the requested search area), are the sort of variables that are ordinarily within a judge's competence to estimate and compare. The same cannot be said of the scope of online searches. Most people—and judges in particular—are unlikely to have a sufficiently expert understanding of online search and search

---

[34] *See supra*, note 73.

[35] See *supra*, note 104. For more on the barriers Google imposes on users who attempt to prevent the company from tracking their location, see: Emily Dreyfuss, *Google Tracks You Even If Location History's Off. Here's How to Stop It*, WIRED (Aug. 13, 2018), https://tinyurl.com/325tt4kp; *Google Found To Track The Location Of Users Who Have Opted Out*, NBC NEWS (Aug. 13, 2018), https://tinyurl.com/ktkchb8y.

[36] *See, e.g.,* 590 F. Supp. 3d at 930; 2020 WL 5491763 at *5 ("As noted *supra*, the geographic scope of this request in a congested urban area encompassing individuals' residences, businesses, and healthcare providers is not 'narrowly tailored' when the vast majority of cellular telephones likely to be identified in this geofence will have nothing whatsoever to do with the offenses under investigation.").

results to estimate just how "reasonable" a particular reverse keyword search warrant might be.[37] At the very least, these kinds of estimates would be far more susceptible to error than the more traditional estimates of time, area, and density involved in geofence searches.

One potential rejoinder to this point is that these issues can be resolved through Google's multi-step process. By this argument, the inability of courts to determine *ex ante*, how many users will be swept into the reverse keyword search does not present a Fourth Amendment problem, because a court can make this determination before de-anonymization. This argument presents several problems. First, as a practical matter, it's not clear that Google and other major tech companies provide truly anonymized information at Step 1.[38] Relatedly, for the reasons listed above, it's not clear that courts have the technological competency to determine whether information has truly been "anonymized" at Step 1.[39] It may be particularly difficult for a court to determine how the information from a reverse keyword search may be combined with other information at law enforcement's disposal to reveal information intended to be outside of the scope of the first stage.[40]

---

[37] Indeed, the courts have often been accused of being significantly "behind the times" when it comes to understanding modern technologies. In 2010, for example, Chief Justice Roberts asked what the difference between a pager and email was. For more on this topic, see: Mary Graw Leary, *The Supreme Digital Divide*, 48 Tex. Tech L. Rev. 65, 71 (2015).

[38] In the *People v. Seymour*, for example, Google provided full IP addresses for each "anonymized" user at Step 1. *See* Motion Hearing Transcript at 105, *People v. Seymour*, No. 21CR20001 (2022) (https://tinyurl.com/y46t9wsb). An IP address can tell you the city, zip code or area code of your ISP, the name of your ISP, and a "best guess" of the latitude and longitude associated with that IP address. *See What You Get With This Tool*, What is My IP Address, http://whatismyipaddress.com. For example, my IP Address reveals my country, state, city, and the ISP associated with my computer (Columbia University). It also reveals the latitudinal and longitudinal coordinates associated with my IP address, which pinpoint a location eight minutes away from my home. Google's policy prohibits them from sharing complete IP addresses at Step 1, although they did so in this case. *See* Motion to Suppress Evidence from a Keyword Warrant & Request for a Veracity Hearing at ¶28, *People v. Seymour*, No. 21CR20001 (2022) (https://tinyurl.com/y46t9wsb).

[39] In fact, the extent to which any anonymization is truly possible, given our expanding data economy, is the subject of debate. *See*, *e.g.,* Gina Kolata, *Your Data Were 'Anonymized'? These Scientists Can Still Identify You*, N.Y. Times (July 23, 2019).

[40] Law enforcement agencies increasingly purchase access to services that aggregate information from data brokers. *See* Bennet Cyphers, *Inside Fog Data Science, the Secretive Company Selling Mass Surveillance to Local Police*,

iv. *Assumptions about Probable Cause are More Difficult to Make with Respect to Search History*

Courts assume (likely rightly) that individuals nearly always have a smart phone on them, and that smartphones are nearly always tracking the location of their owners.[41]

At first, it may seem that Google searches are equally ubiquitous. After all, Google fields 8.5 billion searches per day (99,000 per second).[42] However, it's not clear that individuals engaged in criminal activity are likely to conduct a Google search related to that activity. This potentially lower probability must in turn be discounted by the likelihood that the particular set of terms that an investigator queries in a reverse keyword search warrant are likely to be the ones that an individual engaged in criminal activity would have used. For these reasons, it seems nearly certain that the likelihood of conducting a successful geofence search is higher than the likelihood of conducting a successful reverse keyword search warrant. This in turn suggests that it is less "probable" that the requested evidence (incriminating search history) is in the location to be searched (Google's databases).

d. How might courts Analyze Reverse Keyword Searches

i. Third Party Doctrine and Reverse Keyword Searches

EFF (Aug., 21, 2022); Sharon Bradford Franklin, Greg Nojeim, Dhanaraj Thakur, *Legal Loopholes and Data for Dollars: How Law Enforcement and Intelligence Agencies Are Buying Your Data from Brokers, Center for Democracy and Technology* (Dec. 9, 2021). Frequently, they maintain that use of such services does not implicate any Fourth Amendment issues. Cyphers, *Inside Fog Data Science* ("Troublingly, those records show that Fog and some law enforcement did not believe Fog's surveillance implicated people's Fourth Amendment rights and required authorities to get a warrant."). Access to such resources can augment arguably "anonymized" searches, such as Step 1 of reverse keyword searches or geofence searches.

[41] *Mobile Fact Sheet*, Pew Research Center (April 7, 2021), https://tinyurl.com/yadh2yt4 (finding that 85% of Americans own smartphones).

[42] Maryam Mohsin, *10 Google Search Statistics*, Oberlo: Blog (Jan. 2, 2022), https://tinyurl.com/mwta2acc.

People v. Seymour is currently the only case addressing the use of reverse keyword search warrants. There, law enforcement used a reverse keyword search warrant to identify suspects in an arson investigation.[43] The reverse keyword search identified all users who had searched for the victims' address around the time of the arson.[44]

The Colorado District Court in *Seymour* found that the reverse keyword search at issue required the use of a warrant.[45] In justifying its decision, the court relied on federal law and in the alternative, state constitutional law.[46] Further, the court argued that the *type* of information at issue here was distinct from traditional information shared through the third-party doctrine because of the inescapability of the internet.[47]

Google has largely assumed that other reverse searches (geofence searches), require a warrant, and thus are not covered by the third-party doctrine.[48] In the geofence context, courts have consistently refused to investigate whether *Carpenter* applies—many instead "assume without deciding" that a warrant is required.[49] Google has extended its warrant requirement to the reverse keyword search warrant, and we might expect courts to do the same. If they do, then reverse keyword searches will presumptively require a warrant.

---

[43] Motion Ruling Transcript at 22-23, *People v. Seymour*, No. 21CR20001 (2022) (https://tinyurl.com/34ap8s94); District Court's Response to the Order to Show Cause at 22-24, *People v. Seymour*, No. 21CR20001 (2022) (https://tinyurl.com/bdfw2bsy).

[44] *Id.*

[45] *Id.*

[46] District Court's Response to the Order to Show Cause at 22-24, *People v. Seymour*, No. 21CR20001 (2022) (https://tinyurl.com/bdfw2bsy).

[47] District Court's Response to the Order to Show Cause at 22-23, *People v. Seymour*, No. 21CR20001 (2022) (https://tinyurl.com/bdfw2bsy) ("[T]he U.S. Supreme Court has been hesitant apply the third-party doctrine to digital records… Moreover, this Court has demonstrated a willingness to interpret the state constitution to afford broader protections than its federal counterpart. This is especially true as to the third party doctrine. Splitting with *Miller* and *Smith* respectively, this Court has held that Coloradans maintain a reasonable expectation of privacy under the Colorado Constitution in their financial records, and their telephone records, even though both reside with third parties." (citations omitted)).

[48] *See* Section II.B.i, *supra*, discussing courts' assumptions about whether geofence searches require a warrant.

[49] See *supra*, note 88.

Quite another question is whether reverse keyword search warrants *should* require a warrant. On one hand, reverse keyword searches involve the use of data collected by an internet service most people use almost daily. Even if these individuals are aware the information is being shared with Google, it is doubtful that they expect this information will be subject to invasive search by law enforcement.

However, reverse searches are "wide" rather than "deep" searches, a factor that seems to cut against the applicability of *Carpenter*.[50] They typically do not directly involve location information, which again cuts against the applicability of *Carpenter*. They also involve information that is arguably more consensually given than the CSLI in *Carpenter*, which was collected automatically from anyone who carried a phone. Search history may also be more consensually given than location history, which is collected nearly ubiquitously and very difficult to delete.

Carpenter's frustrating ambiguity sheds little light on the salience of these differences. Reading *Carpenter* narrowly, the differences between search history and location information seem to cut in favor of applying the third-party doctrine to reverse keyword searches. Without further elaboration from the Supreme Court, it's difficult to tell how far the analysis in *Carpenter* should extend.

ii. Probable Cause and Reverse Keyword Searches

As noted in Part II.C.iv, there are differences in the probable cause analysis involved in a geofence search and those involved in a reverse keyword search. Nevertheless, that distinction

[50] 590 F.Supp.3d at 926 (Discussing the validity of geofence warrants: "As this Court sees it, analysis of geofences does not fit neatly within the Supreme Court's existing 'reasonable expectation of privacy' doctrine as it relates to technology. That run of cases primarily deals with deep, but perhaps not wide, intrusions into privacy.").

may turn out to be immaterial. In determining whether a particular piece of information is likely to fall within the parameters of the probable cause requirement, courts have used a "fair probability" standard.[51] Even if the likelihood that an individual involved in criminal activity conducted an online search is lower than the likelihood that an individual involved in criminal activity's location was captured, there is still a "fair" likelihood that the former occurred. After all, the average person uses Google three to four times per day.[52] Most modern queries pass through an online search engine, and 92% of all global searches happen on Google.[53]

Perhaps this kind of bare showing that "most people Google things" will prove insufficient for a finding of probable cause.[54] However, it's not clear that a substantially stronger standard will replace it. In *People v. Seymour*, the Colorado courts found that the government made a sufficient showing of probable cause by arguing that the arson in the case was targeted, rather than random.[55] The government made this showing by arguing that the house was "non-descript," and that arson was a crime of a violent nature.[56] As a result, the state argued, it was likely that the individuals involved in the crime had searched for the address of the targeted home online.[57] At bottom, the standard the state appears to be relying on in *Seymour* is simply that if a crime appears to be pre-

---

[51] 579 F.Supp.3d at 74 (Holding that probable cause and fair probability are synonymous, and further that: "[a]t bottom, probable cause 'is not a high bar.'").

[52] Hazel Emnace, *23 Essential Google Search Statistics*, FIT SMALL BUSINESS (Oct. 25, 2022), https://tinyurl.com/veds8pfr.

[53] *Id.*; A Pew Research Center study found that 46% of surveyed individuals turned to online tools to conduct their research, compared to 25% who said they consulted with others, 8% of individuals who relied on print media, and 11% who relied on prior education. Eric Turner and Lee Rainie, *Most Americans Rely on Their Own Research to Make Big Decisions, And That Often Means Online Searches*, Pew Research Center (Mar. 5, 2020), https://tinyurl.com/nr6bb6am.

[54] Though there is reason to doubt that this will be the case. In the geofencing context, some courts have attempted to circumscribe the probable cause requirement by requiring that the government have evidence that a cellphone was used in the course of the crime. But over time, most courts have dropped this requirement.

[55] District Court's Response to the Order to Show Cause at 29, *People v. Seymour*, No. 21CR20001 (2022) (https://tinyurl.com/bdfw2bsy).

[56] *Id.*

[57] *Id.*

mediated, rather than random, there will be probable cause. This remains a far cry from the constraints of the traditional probable cause inquiry.

iii. Particularity and Reverse Keyword Search Warrants

As noted above, the particularity standard used in geofence search cases seems difficult to import into the geofence context. Geofence cases rely on variables like the size of the area in question, its population density, the time of day and span of time at issue in the search to determine whether a geofence warrant is sufficiently particular. Courts may use a similar strategy for reverse keyword search warrants, for example by evaluating how many terms are used in a particular search, whether the terms themselves are rare or common words, whether the search requires that certain phrases be included or excluded.

Nevertheless, the above-expressed concern remains: It would be difficult for the average person, let alone the average judge, to determine how many hits a search was likely to generate *ex ante*. The lack of judicial competence in this area could lead to two problems: First, that judges apply their own intuitions about the scope of a search *too* liberally, and thus yield varied results across warrant applications, making it difficult to anticipate whether particular activity will be protected. Second, and perhaps more plausibly, judges may understand their limited expertise in this area and apply criteria from previous cases *too* rigidly. Take this stylized example: if another court found twenty terms in a search was sufficiently particular, then the court in question may find that twenty-one terms is *per se* sufficient. This may not lead to the same issues of uncertainty, but it may make the warrant process open to manipulation or inflexible to the point of unfairness.

Particularity, in the context of reverse keyword searches, is the Fourth Amendment requirement with the fewest analogs in existing case law, and thus its application in the reverse keyword search context is difficult to predict. Nonetheless, what *is* foreseeable is that the existing

way in which courts evaluate particularity in the reverse search context cannot be readily imported into this context. Attempts to do so will likely be problematic and insufficiently protective.

e. The Good Faith Exception

Reverse searches have appeared in a moment in Fourth Amendment legal history in which the parameters of constitutional search are in flux.[58] This, of course, is no accident: *Carpenter* is itself the manifestation of a Fourth Amendment scrambling to keep pace with the explosion of digital surveillance tools available to law enforcement in the modern age.[59]

As the preceding pages have demonstrated, Fourth Amendment law is confusing and uncertain, and particularly confusing and uncertain to those subject to reverse search warrants. For criminal defendants against whom reverse keyword searches are used, this uncertainty may even work against them because of the existence of the good faith exception.

The good faith exception holds that where police conduct a search in reliance on a "reasonable and good faith belief that their conduct is lawful," the evidence they collect from said search will not be excluded in later legal proceedings.[60] A line of cases beginning with *United States v. Leon* suggest that if evidence is obtained in a manner that violates the Fourth Amendment, but an officer has not behaved in a "deliberate," "reckless" or "grossly negligent" manner, the evidence will not be excluded.[61] It does not seem likely that a court would characterize a search based on a doctrine rife with uncertainty as "deliberate" or "reckless." Thus, the doctrine's lack of clarity is itself a

---

[58] For further evidence of this constitutional uncertainty, see Tokson, *supra* note 76.

[59] *See* Susan Freiwald & Stephen W. Smith, *The Carpenter Chronicle: A Near-Perfect Surveillance*, 132 HARV. L. REV. 205, 205-6 (2018).

[60] *United States v. Leon*, 468 U.S. 897, 909 (1984) ("Nevertheless, the balancing approach that has evolved in various contexts—including criminal trials—'forcefully suggest[s] that the exclusionary rule be more generally modified to permit the introduction of evidence obtained in the reasonable good-faith belief that a search or seizure was in accord with the Fourth Amendment'").

[61] *Davis v. United States*, 564 U.S. 229, 238 (2011).

shield for officers who conduct novel and under-litigated forms of search, such as the one at issue in this Note.

Furthermore, the highly factual nature of the particularity requirement in these cases (e.g., was the size of the data retrieved too large? Were the search terms sufficiently narrow?) is unlikely to set clear enough precedents for officers to be expected to learn from the invalidation of a reverse keyword search warrant. Therefore, it is unlikely that successive invalidations will have much of an effect on the applicability of the good faith exception in this context.

And while Google (and the courts whose decisions are available to the public) have largely assumed that reverse searches are Fourth Amendment searches requiring a warrant, the preceding analysis demonstrates that that is far from clear. Where a reverse keyword search is conducted without a warrant, law enforcement may rely on the good faith exception to admit evidence that is deemed unconstitutionally obtained. A recent study of courts applying *Carpenter* found that in in nearly 40% of cases where the constitutional validity of a search was at issue, the court never answered the question of whether *Carpenter* applied. [62]

Courts have been slow to take up reverse searches, and where they have taken up such searches, they have consistently failed to explore whether *Carpenter* applies.[63] This approach sustains the murkiness of the doctrine, which in turn makes it easier for challenged law enforcement officers to rely on the good faith doctrine as a defense.

f. Conclusion: The Fourth Amendment Is Insufficiently Protective

---

[62] Tokson, *supra* note 76 at 1809.
[63] Courts have largely assumed without deciding that *Carpenter* applies. *See supra* note 88.

The Fourth Amendment has been decried by myriad scholars and judges as insufficiently protective of privacy interests in the modern world.[64] In the case of reverse keyword search warrants, there is reason to suspect that the Fourth Amendment's protections (such that they are) will not extend to this new search practice. There is also reason to expect that where the Fourth Amendment does apply, its central guardrails—probable cause and particularity—may not be adequately protective of privacy interests. And finally, under the good faith exception, a court finding that a reverse keyword search has been improperly conducted or a warrant for such a search has been improperly issued is unlikely to offer any substantive recourse to present criminal defendants or future ones. The reverse keyword search warrant is a case study in just how ineffectual the Fourth Amendment, without more, can be—and, in particular, what an inadequate safeguard it can be in the face of rapidly advancing technology.

[64] *See* Freiwald and Smith, *supra* note 135 at 205-6 ("On May 24, 1844, a crowd gathered inside the United States Supreme Court chambers in the basement of the Capitol, eagerly awaiting a demonstration of an amazing new communication technology. They watched as inventor Samuel F.B. Morse successfully sent the first long-distance telegraph message—"What hath God wrought?"—to a railroad station near Baltimore.[…] That day may well have marked the last time the Supreme Court was completely in step with modern communication technology").; *See also* Neil Richards, *The Third-Party Doctrine and the Future of the Cloud,* 94 WASH. U.L. REV. 1441, 1447-1465 (2017) (discussing the Fourth Amendment's "lag problem").

Applicant Details

First Name	**Shelby**
Last Name	**Butt**
Citizenship Status	**U. S. Citizen**
Email Address	**seb2243@columbia.edu**
Address	**Address** Street **1930 Broadway - #6B** City **New York** State/Territory **New York** Zip **10023**
Contact Phone Number	**2149129875**

Applicant Education

BA/BS From	**Georgetown University**
Date of BA/BS	**May 2020**
JD/LLB From	**Columbia University School of Law** **http://www.law.columbia.edu**
Date of JD/LLB	**May 22, 2024**
Class Rank	**School does not rank**
Law Review/Journal	**Yes**
Journal(s)	**Columbia Journal of Transnational Law**
Moot Court Experience	**Yes**
Moot Court Name(s)	**Foundational Moot Court**

Bar Admission

Prior Judicial Experience

Judicial Internships/ Externships	**No**
Post-graduate Judicial Law Clerk	**No**

Specialized Work Experience

Recommenders

Rakoff, Jed
Jed_S_Rakoff@nysd.uscourts.gov
Waxman, Matthew
mwaxma@law.columbia.edu
212-854-0592
Richman, Dan
drichm@law.columbia.edu
212-854-9370

This applicant has certified that all data entered in this profile and any application documents are true and correct.

Shelby E. Butt
1930 Broadway, 6B
New York, NY 10023
(214) 912-9875
seb2243@columbia.edu

June 12, 2023

The Honorable Kenneth M. Karas
United States District Court
Southern District of New York
Charles L. Brieant, Jr. United States Courthouse
300 Quarropas Street, Room 533
White Plains, NY 10601-4150

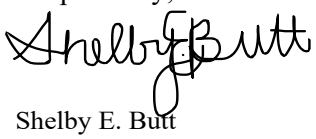
Dear Judge Karas:

I am a rising third-year student, James Kent Scholar, and Executive Online Editor of the *Columbia Journal of Transnational Law* at Columbia Law School. I write to apply for a clerkship in your chambers for the 2025–2026 term. I am particularly interested in clerking for you because of the relatively high number of national security-related cases on your docket.

Enclosed please find my resume, transcript, and writing sample. Also enclosed are letters of recommendation from Professor Matthew C. Waxman (212 854-0592, mwaxma@law.columbia.edu), Professor Daniel C. Richman (212 854-9370, drichm@law.columbia.edu), and the Honorable Jed S. Rakoff of the U.S. District Court for the Southern District of New York (jed_s_rakoff@nysd.uscourts.gov).

Thank you for your time and consideration. Should you need any additional information, please do not hesitate to contact me.

Respectfully,



Shelby E. Butt

SHELBY E. BUTT
1930 Broadway #6B, New York, NY 10023 ● seb2243@columbia.edu ● (214) 912-9875

EDUCATION

Columbia Law School, New York, NY
J.D. expected May 2024
Honors: James Kent Scholar, 2022-2023
Harlan Fiske Stone Scholar, 2021-2022
Activities: *Columbia Journal of Transnational Law*, Executive Online Editor
Teaching Assistant for The Honorable Jed S. Rakoff (Criminal Law), Spring 2023
Research Assistant to Professor Matthew C. Waxman, 2023-2024
National Security Law Society, Co-President

Georgetown University, School of Foreign Service, Washington, DC
B.S.F.S., in International Politics, Minor in Arabic, *cum laude,* received May 2020
Honors: Collegiate Rowing Coaches' Association Scholar-Athlete Award, 2017
Varsity Letter Winner, May 2020
Activities: Varsity Women's Lightweight Crew (NCAA Division I)
Georgetown Undergraduate Scholars Program, Undergraduate Research Scholar
Kappa Alpha Theta, Scholarship Director and Executive Recruitment Board

EXPERIENCE

Williams & Connolly, Washington, DC — Summer 2023
Summer Associate
Researched and wrote memoranda on criminal forfeiture law, TILA claims, and qui tam suits. Drafted a motion in limine to exclude expert testimony in a federal criminal fraud case. Worked with attorneys to develop case strategy and provide litigation counseling to clients on white collar civil and criminal matters.

U.S. Attorney's Office for the Eastern District of New York, Brooklyn, NY
Intern, Criminal Division — Summer 2022
Supported AUSAs in the National Security & Cybercrime and International Narcotics & Money Laundering divisions by drafting sentencing memos, conducting legal research, reviewing evidence, and assisting with trial prep. Spoke on behalf of the U.S. government in court proceedings under the guidance of experienced prosecutors.

Entegra Systems, Langley, VA
Intelligence Officer (Level 1) — July 2020 - June 2021
Served as a Desk Officer for a U.S. Government client within the U.S. Intelligence Community (IC). Trained in IC style cable-writing, case study analysis, and short form briefing. Maintained an active TOP SECRET/Sensitive Compartmented Information (TS/SCI) security clearance issued by the U.S. Department of Defense.

Council on Foreign Relations, Washington, DC
Intern for Middle East and U.S. Foreign Policy — Spring 2020
Edited and fact checked quotes, anecdotes, and references in CFR publications. Conducted research and wrote memos on the Qatar Crisis, Russia-Saudi Arabia oil price war, and ISIS in Syria to prepare CFR personnel for round table meetings and congressional testimonies.

National Security Agency, Fort Meade, MD
Intelligence Analysis Intern — Summer 2019
Attained knowledge and skills in signals intelligence (SIGINT) and intelligence analysis through work in the NSA's Directorate of Operations. Obtained a TS/SCI security clearance. Presented a final project and methodology paper to NSA senior leadership and received the Internship Spotlight Award for outstanding work.

LANGUAGE SKILLS: Spanish (proficient), Arabic (intermediate), Russian (basic), French (basic)
PUBLICATIONS: Shelby Butt and Daniel Byman. "Right-Wing Extremism: The Russian Connection." *Survival*, vol. 62, no. 2, 2020, pp. 137–52.
VOLUNTEER WORK: Georgetown Alumni Admissions Interviewer (2020-Present), Phillips Academy Andover Class Agent (2016-Present).
INTERESTS: Documentary films, foreign languages, and running with Bella, my three-year-old German shepherd.

Columbia Law School

Registration Services

law.columbia.edu/registration
435 West 116th Street, Box A-25
New York, NY 10027
T 212 854 2668
registrar@law.columbia.edu

CLS TRANSCRIPT (Unofficial)

06/07/2023 23:09:14

Program: Juris Doctor

Shelby E Butt

Spring 2023

Course ID	Course Name	Instructor(s)	Points	Final Grade
L6241-1	Evidence	Capra, Daniel	4.0	A
L6429-1	Federal Criminal Law	Richman, Daniel	3.0	A-
L9327-1	S. Internet and Computer Crimes [Minor Writing Credit - In Progress]	DeMarco, Joseph; Komatireddy, Saritha	2.0	A
L6683-1	Supervised Research Paper	Waxman, Matthew C.	1.0	CR
L6822-1	Teaching Fellows	Rakoff, Jed	3.0	CR

Total Registered Points: 13.0

Total Earned Points: 13.0

Fall 2022

Course ID	Course Name	Instructor(s)	Points	Final Grade
L6238-1	Criminal Adjudication	Richman, Daniel	3.0	A-
L6169-2	Legislation and Regulation	Menand, Lev	4.0	A
L6675-1	Major Writing Credit	Waxman, Matthew C.	0.0	CR
L6274-2	Professional Responsibility	Fox, Michael Louis	2.0	A
L8951-1	S. Cybersecurity, Data Privacy and Surveillance Law	Richman, Daniel; Tannenbaum, Andrew; Waxman, Matthew C.	2.0	A
L6683-1	Supervised Research Paper	Waxman, Matthew C.	1.0	CR

Total Registered Points: 12.0

Total Earned Points: 12.0

Spring 2022

Course ID	Course Name	Instructor(s)	Points	Final Grade
L6133-2	Constitutional Law	Ponsa-Kraus, Christina D.	4.0	A-
L6108-3	Criminal Law	Rakoff, Jed	3.0	A
L6679-1	Foundation Year Moot Court		0.0	CR
L6121-20	Legal Practice Workshop II	Statsinger, Steven	1.0	P
L6116-3	Property	Heller, Michael A.	4.0	A-
L6912-1	Transnational Litigation	Smit, Robert	3.0	A

Total Registered Points: 15.0

Total Earned Points: 15.0

January 2022

Course ID	Course Name	Instructor(s)	Points	Final Grade
L6130-6	Legal Methods II: International Problem Solving	Hakimi, Monica	1.0	CR

Total Registered Points: 1.0

Total Earned Points: 1.0

Fall 2021

Course ID	Course Name	Instructor(s)	Points	Final Grade
L6101-3	Civil Procedure	Johnson, Olatunde C.A.	4.0	A-
L6105-5	Contracts	Arato, Julian	4.0	B
L6113-1	Legal Methods	Ginsburg, Jane C.	1.0	CR
L6115-20	Legal Practice Workshop I	Statsinger, Steven; Yoon, Nam Jin	2.0	P
L6118-2	Torts	Merrill, Thomas W.	4.0	B+

Total Registered Points: 15.0

Total Earned Points: 15.0

Total Registered JD Program Points: 56.0

Total Earned JD Program Points: 56.0

Honors and Prizes

Academic Year	Honor / Prize	Award Class
2022-23	James Kent Scholar	2L
2021-22	Harlan Fiske Stone	1L

Pro Bono Work

Type	Hours
Mandatory	40.0
Voluntary	7.0

UNITED STATES DISTRICT COURT
UNITED STATES COURTHOUSE
500 PEARL STREET
NEW YORK, NEW YORK 10007

JED S. RAKOFF
UNITED STATES DISTRICT JUDGE

May 5, 2023

Re: Shelby E. Butt

Dear Judge:

This letter is written in my capacity as a long-time professor at Columbia Law School to enthusiastically recommend my teaching assistant Shelby Butt for a position as your law clerk. As the rest of this letter will demonstrate, Shelby has every quality needed to be an outstanding law clerk. Indeed, it is only because of my strict and long-standing policy against offering a clerkship to anyone who serves as my teaching assistant that I cannot grab her for my own law clerk!

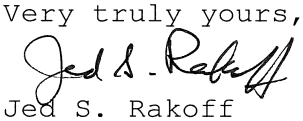
Shelby is a classic case of someone who took a little while to get the "feel" of the law (- her initial grades her first semester were mixed -), but, once she did, not only achieved outstanding grades but also demonstrated that she had a brilliant legal mind. I know this first hand, because Shelby was a student her second semester in my Criminal Law class, a huge class of over 105 students where it would be easy to "disappear." But not Shelby! Not only did she give great answers when called upon in class, but also she turned in a near-perfect exam that put her at the very very top of the class - and led me to ask her to be my teaching assistant this year.

I expect a lot of my T.A.'s: teaching weekly review sessions, devising hypotheticals for each class, grading midterm exams, meeting with students individually, devoting substantial time to those students needing extra help, etc., etc. Shelby not only met this challenge - executing every aspect of the job in a helpful, indefatigable, and totally successful way - but did so with such warmth and conscientiousness that she was a great favorite with my students (and with me).

As you will see from Shelby's resume, she is also a very broad-based person with a wide variety of prior experiences that will make her even more an asset to your chambers. Among much else, before coming to law school, she served for a year as a U.S. intelligence officer and co-authored an excellent published article on the rise of far-right extremism in Russia. At the same time, she is totally down-to-earth, unpretentious, and a pleasure to work with.

In short, Shelby is both a marvelous person and a great student of the law, and has every quality needed to be a superb law clerk. I recommend her most highly!

Very truly yours,



Jed S. Rakoff

June 11, 2023

The Honorable Kenneth Karas
Charles L. Brieant, Jr. United States Courthouse
300 Quarropas Street, Room 533
White Plains, NY 10601-4150

Dear Judge Karas:

Clerkship Recommendation for Shelby Butt

I have worked closely with Shelby Butt inside and outside the classroom, and I know she will make a superb clerk.

During the Fall of her 2L year, Shelby was a top student in my seminar on Cybersecurity, Data Privacy and Surveillance Law. Additionally, I advised Shelby on the Note she wrote for the Columbia Journal of Transnational Law (CJTL). Titled Old Laws and New Tricks: Interpreting Existing Legal Authorities to Regulate the Data Brokerage Industry. Her Note proposed using existing export-control regulations to circumscribe the sale of U.S. persons' sensitive personal data to foreign entities and individuals. Her work in the seminar and on the Note dis-played outstanding research, writing, and analytical skills--including very careful and thoughtful parsing of difficult statutory, regulatory, and legislative history materials. She has all the makings of a terrific lawyer. Indeed, her work has been so outstanding that I have recruited her to serve next year as my research assistant.

Shelby has a sterling transcript--she is virtually a lock for some of our highest academic honors--and she is a leader in the Columbia Law School community, including serving as co-president of the National Security Law Society (I am a faculty advisor to that student group, so I had the great fortune of working with her to organize several terrific events and programs). Testifying further to the high regard in which her classmates hold her, Shelby now serves on the editorial board of the Columbia Journal of Transnational Law. As a highly-accomplished former scholar-athlete, she brings great energy to all her pursuits.

Shelby's professional experience to date shows her deep and longstanding interest in public service, and she hopes to pursue a career as a federal prosecutor or government attorney. I have been immensely impressed with Shelby's skills, intellect and work ethic and I know she will be a superb clerk and stellar public servant.
I highly recommend this outstanding candidate.

Sincerely,

Matthew Waxman

Liviu Librescu Professor of Law
Faculty Chair of the National Security Law Program

Matthew Waxman - mwaxma@law.columbia.edu - 212-854-0592

COLUMBIA LAW SCHOOL
435 West 116th Street
New York, NY 10027

June 10, 2023

The Honorable Kenneth Karas
Charles L. Brieant, Jr. United States Courthouse
300 Quarropas Street, Room 533
White Plains, NY 10601-4150

Re: Shelby Butt

Dear Judge Karas:

I write to enthusiastically support the application of Shelby Butt — a rising Columbia Law School 3L, Class of 2024 — to clerk in your Chambers. She has a keen intelligence, excellent writing skills, wonderful organizational and leadership abilities, and a commitment to public service that together – and coupled with her determined and calm personality – would equip her perfectly for the job.

I've seen quite a lot of Shelby during her 2L year. In the Fall, she took my Criminal Adjudication course and the seminar on Cybersecurity, Data Privacy, and Surveillance Law that I teach with my colleagues Matt Waxman and Andrew Tannenbaum. And in the Spring, she took (and did exceedingly well in) my Federal Criminal Law course. I've also had numerous office conversations with Shelby about course materials, her deep national security law interests, and her future.

Every contact I'm had with Shelby has left me enormously impressed with her cutting intellect, excellent judgment and enormous discipline. In class, her contributions have invariably been thoughtful and insightful. Never flashy, Shelby choses her words carefully and always gets to the heart of the matter. She also writes beautifully and cleanly, and for the cyber seminar, wrote a terrific paper on regulating the data brokerage industry. Even as Congress and state authorities start (fitfully) to come to grips with that vast, virtually unregulated industry, Shelby explored how, at least when it comes to the sale of US persons' data to foreign entities, the Export Control Reform Act of 2018 (ECRA) and the Export Administration Regulations (EAR) provide some basis for Commerce Department intervention. It was a masterful piece of thorough analysis, at the cutting edge of regulatory possibility, and powerful evidence of Shelby's ability to work though a new and complex regulatory framework in service of privacy and national security concerns.

Shelby's interest in national security matters is broad and deep. She went to Georgetown's Walsh School of Foreign Service, drawn by her interest in the Middle East and her desire to pursue a career in the Intelligence Community. She spent the summer before her senior year as a "token non-STEM hire" at the NSA (in Operations) and developed sufficient technical expertise to be offered a fulltime job there after graduation. She turned that down however, and, having more interest in human source collection, was about to start as an Operations Officer at CIA, when COVID intervened and delayed her clearance process. She used this time to attend Russian language school and improve her Arabic dialects, but also to reconsider her career choice and see law school as a way to continue to work in national security in new settings. The events of January 6 only confirmed her decision. She writes: "Turning down the opportunity to become a CIA Operations Officer is the hardest decision I've made to date, but a J.D. would only help me in a career protecting the people and Constitution of the United States, especially when some of the biggest threats are coming from within the country's own borders."

The meaningful work Shelby got to do during 1L summer at the EDNY USAO solidified her ambition to be an AUSA. She certainly has the judgment, intellect, and decency to be a terrific prosecutor – I just need her to speak a little more loudly. She's working on that, and what Shelby works on she succeeds at. I wasn't surprised to learn that she was a varsity lightweight rower at Georgetown, as discipline, time-management and dedication are foundational to the way she engages with the world.

With her cutting intelligence, hyper-competence, common sense, and commitment to public service, I expect great things of Shelby. I am also confident that she would be an extraordinary law clerk, a delight to work with and a career to watch. If there is anything else I can add, please give me a call.

Respectfully yours,

Daniel Richman

Dan Richman - drichm@law.columbia.edu - 212-854-9370

SHELBY E. BUTT
Columbia Law School J.D. '24
214-912-9875
seb2243@columbia.edu

CLERKSHIP APPLICATION WRITING SAMPLE

This writing sample is a paper I wrote for a course titled L9327-1: Seminar on Internet and Computer Crimes. The course considered how crimes committed in cyberspace challenge traditional investigatory and prosecutorial tools and covered topics such as the Fourth Amendment in cyberspace, the law of electronic surveillance, computer hacking, computer viruses, and cyberterrorism. Students were required to write two 2,000-word papers on a topic of their choice related to one of the issues discussed in class, and I wrote about the prospect of using the Computer Fraud and Abuse Act to prosecute Zoom-bombings, a cyber-harassment technique that gained popularity during the Covid-19 pandemic. I revised this paper in response to high-level feedback received from my seminar professor before submitting it as a writing sample.

THE POTENTIAL FOR CFAA PROSECUTIONS OF ZOOM-BOMBINGS

Introduction

Zoom-bombing refers to the unwanted disruption of any video conference, usually by an uninvited participant using the platform's screensharing function to project racist, hateful, or pornographic material onto the screens of other meeting participants.[1] The practice gained popularity during the Covid-19 pandemic when many were forced to substitute virtual meetings for in-person events.[2] Since March 2020, Zoom-bombing incidents have impacted online classes,[3] Alcoholics Anonymous meetings,[4] religious services, and countless other virtual gatherings, often targeting meetings based on the identity of their participants.[5]

Because Zoom-bombing is a relatively new form of cybercrime, no federal or state statutes explicitly criminalize it. This leaves prosecutors the task of figuring out which, if any, existing statutes can be used to prosecute it. During the early days of the pandemic, the U.S. Attorney's Office for the Eastern District of Michigan indicated that Zoom-bombing could be prosecuted as a federal crime.[6] Although not explicitly cited in their press release, the Computer Fraud and Abuse Act (CFAA) is the federal statute most readily suited for this task because it provides a general prohibition against computer misuse.[7] As the rest of this paper demonstrates,

---

[1] Taylor Lorenz, *'Zoombombing': When Video Conferences Go Wrong*, N.Y. TIMES (Mar. 20, 2020), https://www.nytimes.com/2020/03/20/style/zoombombing-zoom-trolling.html.
[2] FED. BUREAU INVESTIGATION, *FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic* (Mar. 30, 2020), https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic.
[3] *Id.*
[4] Taylor Lorenz & Davey Alba, *'Zoombombing' Becomes a Dangerous Organized Effort*, N.Y. TIMES (Apr. 7, 2020), https://www.nytimes.com/2020/04/03/technology/zoom-harassment-abuse-racism-fbi-warning.html.
[5] *What is "Zoombombing" and Who is Behind It?*, ANTI-DEFAMATION LEAGUE (May 4, 2020), https://www.adl.org/resources/blog/what-zoombombing-and-who-behind-it.
[6] *Federal, State, and Local Law Enforcement Warn Against Teleconferencing Hacking During Coronavirus Pandemic*, DEPT. JUST. (Apr. 3, 2020), https://www.justice.gov/usao-edmi/pr/federal-state-and-local-law-enforcement-warn-against-teleconferencing-hacking-during.
[7] ORIN S. KERR, COMPUTER CRIME LAW 30 (5th ed., 2022). Although several states have their own cybercrime statutes, this paper will focus on the CFAA and federal case law.

the ability to prosecute Zoom-bombing under the CFAA is highly dependent on the facts of the case and relevant jurisdiction's case law, and attacks on password-protected meetings are more likely to be prosecutable under the CFAA.

The Computer Fraud and Abuse Act – 18 U.S.C. § 1030

The CFAA outlines seven categories of prohibited behavior, but § 1030(a)(2)(C) is most useful for prosecuting Zoom-bombing because it "prohibits accessing a computer without authorization . . . and obtaining information [from it]."[8] To prosecute an individual under § 1030(a)(2)(C), "the Government must prove that the defendant (1) intentionally (2) accessed without authorization . . . a (3) protected computer and (4) thereby obtained information [from it]."[9] To assess the potential for prosecuting Zoom-bombings under the CFAA, each of these elements will be evaluated below.

Element One: "Intentionally"

Section 1030(a)(2)(C)'s first and third elements are easily satisfied in the context of Zoom-bombing. Intentionality, the first element, is shown by the steps a Zoom-bomber must take to carry out an attack, including clicking on the meeting's access link, typing in a password (if required), and instructing his computer to share the offensive content from his screen to those of the other participants. This multi-step process leaves little room for a defendant to argue he lacked intentionality because he took a series of specific steps to cause the ultimate result – the Zoom-bombing.

[8] *Id*. Note that § 1030(a)(2)(C) also prohibits "exceed[ing] authorized access" to a computer, but "access without authorization" is more useful in the context of Zoom-bombing and will be the focus of this paper.
[9] United States v. Auernheimer, 748 F.3d 525, 533 (3d Cir. 2014).

Additionally, some Zoom-bombings are carried out by organized groups that coordinate their attacks using virtual message boards like Reddit and 4Chan.[10] Evidence that a defendant engaged in planning a coordinated Zoom-bombing on one of these websites would make it even more difficult for him to argue he did not act intentionally because any statements he made to others when planning the attack would memorialize his specific intent to carry it out.

Element Three: "Protected Computer"

Like its intentionality requirement, the CFAA's broad definition of "protected computer" makes the third element of § 1030(a)(2)(C) easy to meet in the context of Zoom-bombing. The statute defines "protected computer" to include "any device for processing or storing data . . . [that is] used in or affecting interstate or foreign commerce or communication."[11] In practice, courts have interpreted this provision to cover any computer that connects to the Internet.[12] Since Zoom and other teleconferencing platforms require an Internet connection to function, the CFAA's third element will inevitably be met in any Zoom-bombing prosecution.

Additionally, under current CFAA case law, the defendant does not have to directly access the victim's computer to meet the "protected computer" requirement because courts have found other technological connections between the defendant and victim to satisfy this requirement. For example, courts have found a defendant accessing a victim's website sufficient to meet the CFAA's "protected computer" requirement because websites are hosted by the victim's computer server, so anyone who accesses a website also connects to the server.[13] Like websites, Zoom and other videoconferencing platforms facilitate virtual meetings amongst

[10] Lorenz, *supra* note 4.
[11] 18 U.S.C. § 1030(e)(1)–(2)(B).
[12] *See* United States v. Yücel, 97 F. Supp. 3d 413, 418–419 (S.D.N.Y. 2015) (collecting cases).
[13] hiQ Labs, Inc. v. LinkedIn Corp., 31 F.4th 1180, 1195 (9th Cir. 2022).

individual computers by connecting them through the parent company's servers. Thus, just as a defendant accessing a website by connecting with its server satisfies the CFAA's "protected computer" requirement, a Zoom-bomber accesses a "protected computer" by connecting to the platform's server when joining the virtual meeting to carry out his attack.[14]

Element Two: "Access Without Authorization"

The CFAA's second element is more challenging to meet in the context of Zoom-bombing, though attacks targeting password-protected meeting may constitute "access[] without authorization" under the statute.[15] The CFAA does not define "access" or "authorization," but recent case law provides guidance on their contours in the Zoom-bombing context. In *Van Buren v. United States*, the Supreme Court interpreted "access" as used in the CFAA to mean "the act of entering a computer system itself."[16] Since post-*Van Buren* cases continue to hold websites are "protected computers,"[17] a Zoom-bomber's entrance into a virtual meeting will constitute "access" under the statute, even if he does not enter the meeting participants' computers themselves.

The "without authorization" portion of § 1030(a)(2)(C) makes the biggest difference in determining which Zoom-bombings fall within the CFAA's scope because courts have generally interpreted "without authorization" to mean the defendant accessed the computer, website, or software program without permission.[18] For password-protected virtual meetings, the

[14] ZOOM VIDEO COMMS., *Connection Process*, https://explore.zoom.us/docs/doc/Zoom%20Connection%20Process%20Whitepaper.pdf (last accessed Feb. 21, 2022) ("A Zoom Meeting Zone is a logical association of servers that are physically co-located that can host a Zoom session.").
[15] § 1080(a)(2)(C).
[16] 141 S. Ct. 1648, 1658 (2021).
[17] *See hiQ Labs*, 31 F.4th at 1195.
[18] *Id.*

defendant's lack of permission in accessing the meeting is easy to show if he hacks into the meeting, bypassing any password requirement.[19] Additionally, case law indicates a Zoom-bomber who accesses a meeting using a legitimate password that he himself was not authorized to use could violate the CFAA, even though he did not circumvent the meeting's password requirement.[20] This could happen if the Zoom-bomber knows one of the meeting's participants, asks that person for the meeting password, logs into the meeting using it, and then carries out the Zoom-bombing attack. In at least the Ninth Circuit, this conduct would violate the CFAA because the perpetrator himself was not authorized to use the meeting password, so his use of it to enter the meeting is still "without authorization" even though the password itself is correct.

Access "without authorization" is harder to prove for non-password-protected meetings because the defendant's ability to enter the virtual meeting without circumventing a password requirement makes the meeting akin to a public-facing website, which some courts have held cannot be accessed "without authorization" due to their lack of limitations on access.[21] Other courts, however, have held that a website's lack of password protection does not render it completely without access requirements, especially when the material featured on the website is sensitive in nature and the defendant knows the website link is not publicly distributed.[22] This could be helpful for prosecutors in situations where the Zoom meeting itself is not password-protected but the link to it is not publicly distributed. For example, in a case where the non-password-protected virtual meeting link is shared amongst friends and the defendant somehow obtains the link and accesses the meeting to carry out a Zoom-bombing, a prosecutor could argue

[19] *See* United States v. Phillips, 477 F.3d 215, 220–221 (5th Cir. 2007) (where a defendant's use of a "brute-force" computer program to access a university's computer system constituted access "without authorization.").
[20] *See* United States v. Nosal, 844 F.3d 1024, 1038 (9th Cir. 2016).
[21] *hiQ Labs*, 31 F.4th at 1180.
[22] Vox Mktg. Grp. v. Prodigy Promos, 556 F. Supp. 3d 1280, 1287 (D. Utah 2021).

the link's non-public nature indicated to the defendant that he lacked authorization to enter the meeting, even if he did not have to circumvent a password requirement to do so.

Alternatively, the prosecution could argue that the Zoom-bomber's conduct once inside the non-password-protected meeting violated the platform's terms of service, which prohibit the display of hateful conduct, violent content, and pornography, making his use of the platform unauthorized.[23] However, this argument will likely fail because most courts have declined to find violating a website's terms of service sufficient to trigger CFAA liability, citing due process concerns like lack of notice and the negative public policy implications of turning minor, everyday computer violations, like using a work computer to check personal email, into federal crimes.[24]

Element Four: "Obtains Information"

Legislative history and subsequent case law indicate that the standard for showing a defendant "obtain[ed] information" under § 1030(a)(2)(C) is low and will be satisfied "whenever a person using a computer contacts an Internet website and [his computer] reads any response from that site."[25] In the context of Zoom-bombing, this fourth element is likely satisfied by the perpetrator clicking on the meeting link to request access to the virtual meeting, his request being transmitted through the Internet to Zoom's server, and the signal granting him access to the meeting being transmitted from the server back to his computer. The meeting being password-protected could also bolster the prosecution's argument that the defendant "obtained information" from Zoom's server because the Zoom-bomber's submission of the password to the

[23] *See* ZOOM, *Acceptable Use Guidelines*, https://explore.zoom.us/en/acceptable-use-guidelines/ (last accessed Feb. 21, 2023).
[24] *See hiQ Labs*, 31 F.4th at 1180; Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1068 (9th Cir. 2016); Sandvig v. Barr, 451 F. Supp. 3d 73, 87 (D.D.C. 2020).
[25] United States v. Drew, 259 F.R.D. 449, 457–458 (C.D. Ca. 2009).

server and the server granting him access to the meeting is an even clearer instance of the defendant's computer contacting the server and reading a response from it.

Conclusion

The ability to prosecute a Zoom-bombing attack using the CFAA is highly dependent on the facts of the case and the relevant court's case law. Zoom-bombings of password-protected meetings likely can be prosecuted under the CFAA because they meet the requirements of § 1030(a)(2)(C) as interpreted in current case law, but non-password-protected meetings are less likely to do so. In particular, proving access "without authorization" for non-password-protected meetings is challenging given many courts' presumption that websites viewable without a password cannot be accessed "without authorization."

Although the CFAA may not apply to all instances of Zoom-bombing, state computer crime laws or federal laws prohibiting the content shared by the Zoom-bomber, like those criminalizing the possession and dissemination of child pornography, may prove useful in prosecuting Zoom-bombings of non-password-protected meetings. These alternative grounds for prosecution are important because not all meeting hosts can realistically use restrict access to their meetings by implementing password protection or not publicly distributing the meeting link. For example, in some States, meetings implicating a public interest, such as townhalls or school board meetings, are required to be open to the public,[26] and many religious services and support groups, like Alcoholics Anonymous, likely want their meetings to remain publicly accessible to encourage potential members to join. Even if CFAA charges cannot be brought in these situations, prosecuting a Zoom-bombing incident under a different statute is the best route

[26] *See* N.Y. STATE SCH. BD. ASS'N, PUBLIC COMMENT GUIDE, https://www.nyssba.org/clientuploads/nyssba_pdf/Events/get-to-know-nyssba-07142021/NYSSBA_FAQ_Public_Comment_5520.pdf (last accessed Feb. 21, 2023).

to punish to perpetrator and deter against future attacks while keeping these virtual meetings open to all.

Applicant Details

First Name	**Joshua**
Middle Initial	**E**
Last Name	**Zakharov**
Citizenship Status	**U. S. Citizen**
Email Address	**jez8239@nyu.edu**
Address	**Address** Street **2621 Palisade Ave, Apt. 9J** City **Bronx** State/Territory **New York** Zip **10463** Country **United States**
Contact Phone Number	**7186441721**

Applicant Education

BA/BS From	**University of Chicago**
Date of BA/BS	**June 2020**
JD/LLB From	**New York University School of Law** **https://www.law.nyu.edu**
Date of JD/LLB	**May 22, 2024**
Class Rank	**School does not rank**
Law Review/Journal	**Yes**
Journal(s)	**New York University Law Review**
Moot Court Experience	**No**

Bar Admission

Prior Judicial Experience

Judicial Internships/Externships	**Yes**

Post-graduate Judicial Law Clerk	**Yes**

Specialized Work Experience

Recommenders

Murphy, Liam
liam.murphy@nyu.edu
212-998-6160

Alvarez, Jose
jose.alvarez@nyu.edu
(212) 992-8835

Issacharoff, Samuel
samuel.issacharoff@nyu.edu
212.998.6580

This applicant has certified that all data entered in this profile and any application documents are true and correct.

June 12, 2023

The Honorable Kenneth Karas
Charles L. Brieant, Jr. United States Courthouse
300 Quarropas Street, Room 533
White Plains, NY 10601-4150

Dear Judge Karas:

I am writing to express my interest in clerking in your chambers during the 2025-26 term. I am a rising 3L at New York University School of Law, where I serve as Articles Editor on the *N.Y.U. Law Review* and was designated one of the top ten students in the class by GPA after 1L and 2L. I currently work at Covington & Burling in Washington, D.C. as a summer associate. After graduating, I will clerk for Judge Anthony J. Scirica on the United States Court of Appeals for the Third Circuit.

Letters of recommendation and contact information will follow from NYU for Professor Samuel Issacharoff, Professor Liam Murphy, and Professor Jose Alvarez. I was a research assistant for Professor Issacharoff and took his Procedure course in 1L and Complex Litigation course in 2L. I was a teaching assistant for Professor Murphy in 2L and took his Contracts course in 1L. I was also a teaching assistant for Professor Alvarez in 2L and took his International Law course in 1L.

The following are also willing to speak as references. I am currently a research assistant for Professor Samuel Rascoff and took his Intelligence course in 2L. Camilla Macpherson is Head of Secretariat of P.R.I.M.E. Finance, the international arbitration organization in The Hague where I interned during the summer after 1L. Nicholaus Mills is a law clerk to Judge Rachel P. Kovner, to whom I reported when I was an extern in Judge Kovner's chambers in the autumn of 2L. Their contact information is as follows:

Samuel Rascoff: samuel.rascoff@nyu.edu; (917) 861-3019
Camilla Macpherson: c.macpherson@primefinancedisputes.org; +44 7442 594 495 (United Kingdom)
Nicholaus Mills: ncm56@cornell.edu; (704) 359-7216

My resume, transcript, and writing sample are attached. Thank you very much for your consideration and I look forward to hearing back. If any further information is needed concerning my application, please let me know.

Respectfully,
/s/ Joshua Zakharov

JOSHUA E. ZAKHAROV
2621 Palisade Ave, Apt. 9J, Bronx, NY 10463
(718) 644-1721
zakharov@nyu.edu

EDUCATION

NEW YORK UNIVERSITY SCHOOL OF LAW, New York, NY
Candidate for J.D., May 2024
Unofficial GPA: 3.963
Honors: Pomeroy Scholar (one of ten students with the top cumulative grades after 1L)
Butler Scholar (one of ten students with the top cumulative grades after 2L)
New York University Law Review, Articles Editor
Institute for International Law and Justice Joyce Lowinson Scholar (merit scholarship)
Activities: Research Asst., Prof. Issacharoff (Summer '22); Center for Civil Justice (Spring '23)
Teaching Asst., Prof. Murphy, Contracts (Fall '22); Prof. Alvarez, Int'l Law (Spring '23)
NYU Trial Advocacy Society (mock trial competition team), External Partnerships Chair

UNIVERSITY OF CHICAGO, Chicago, IL
B.A. Public Policy Studies, B.A. Political Science, *magna cum laude*, June 2020
Senior Thesis: *The Scandinavian Exception to the Law and Finance School*
Honors: Departmental Honors in Public Policy and Political Science
Activities: Vice President, Chicago Debate Society
Research Assistant to Prof. Robert Pape, Chicago Project on Security and Threats

EXPERIENCE

THE HON. ANTHONY J. SCIRICA, U.S. COURT OF APPEALS, THIRD CIRCUIT, Philadelphia, PA
Judicial Law Clerk, August 2024 – August 2025 (expected)

COVINGTON & BURLING LLP, Washington, DC
Summer Associate, May 2023 – July 2023 (expected)
Staffed to matters in regulatory enforcement, class actions, white collar and investigations, and CFIUS.

THE HON. RACHEL P. KOVNER, U.S. DISTRICT COURT, E.D.N.Y., New York, NY
Judicial Extern, August 2022 – December 2022
Drafted memoranda, oral rulings, and opinions. Provided research and review for clerks' drafts. Worked on matters including bankruptcy and SSA appeals, immigration, habeas, and FCA.

KALIKOVA & ASSOCIATES, Bishkek, Kyrgyzstan
Summer Associate, July 2022 – August 2022
Wrote guide for IFIs and foreign investors. Drafted memos on mens rea and jurisdiction for international dispute.

PANEL OF RECOGNIZED INTERNATIONAL MARKET EXPERTS IN FINANCE, The Hague, Netherlands
Summer Legal Intern, May 2022 – July 2022
Contributed to World Bank project on derivatives market development, edited commentary on P.R.I.M.E. Arbitration Rules, proposed changes to P.R.I.M.E. Mediation Rules. Represented P.R.I.M.E. at UNCITRAL meeting at the UN.

U.S. DEPARTMENT OF STATE, Tashkent, Uzbekistan
Fulbright Award, January 2021 – July 2021
Placed at Academy of the General Prosecutor's Office of Uzbekistan and Uzbekistan State World Languages Univ. as English Teaching Assistant. Organized legal English seminars for staff, students at Prosecutor's Academy; assisted comparative law research and translation. Led debate, reading, speaking clubs, taught first-year English at UzSWLU.

DELOITTE, New York, NY
Consultant, Global Trade Advisory, August 2020 – January 2021
Advised clients on business implications of trade policy. Researched bills of lading for forced labor investigations. Briefed CBP administrative rulings to advise clients on import matters. Supported A&D clients on export licensing.

ADDITIONAL INFORMATION

Conversational in Russian and French. Hobbies include speed chess, guitar, table tennis, and coaching debate.

Name: **Joshua E Zakharov**
Print Date: **06/07/2023**
Student ID: **N15764509**
Institution ID: **002785**
Page: **1 of 1**

New York University
Beginning of School of Law Record

Fall 2021

School of Law
Juris Doctor
Major: Law

Lawyering (Year)	LAW-LW 10687	2.5	CR
Instructor: Juan P Caballero			
Criminal Law	LAW-LW 11147	4.0	A
Instructor: Rachel E Barkow			
Torts	LAW-LW 11275	4.0	A-
Instructor: Christopher Jon Sprigman			
Procedure	LAW-LW 11650	5.0	A+
Instructor: Samuel Issacharoff			
1L Reading Group	LAW-LW 12339	0.0	CR
Instructor: James F Gilligan, David A J Richards, Maegan F Ciolino			

	AHRS	EHRS
Current	15.5	15.5
Cumulative	15.5	15.5

Spring 2022

School of Law
Juris Doctor
Major: Law

Lawyering (Year)	LAW-LW 10687	2.5	CR
Instructor: Juan P Caballero			
Legislation and the Regulatory State	LAW-LW 10925	4.0	A
Instructor: Emma M Kaufman			
International Law	LAW-LW 11577	4.0	A+
Instructor: Jose E Alvarez			
Contracts	LAW-LW 11672	4.0	A
Instructor: Liam B Murphy			
Financial Concepts for Lawyers	LAW-LW 12722	0.0	CR

	AHRS	EHRS
Current	14.5	14.5
Cumulative	30.0	30.0

Pomeroy Scholar-Top Ten Students in the first year class

Fall 2022

School of Law
Juris Doctor
Major: Law

Comp Constitutional Law	LAW-LW 10221	2.0	A
Instructor: Tarunabh Khaitan			
Teaching Assistant	LAW-LW 11608	2.0	CR
Instructor: Liam B Murphy			
Constitutional Law	LAW-LW 11702	4.0	A-
Instructor: Kenji Yoshino			
Federal Judicial Practice Externship	LAW-LW 12448	3.0	CR
Instructor: Michelle Beth Cherande, Alison J Nathan			
Federal Judicial Practice Externship Seminar	LAW-LW 12450	2.0	CR
Instructor: Michelle Beth Cherande, Alison J Nathan			
Research Assistant	LAW-LW 12589	1.0	CR
Summer 2022 Research Assistant			
Instructor: Samuel Issacharoff			
Class Actions Seminar	LAW-LW 12721	2.0	A-
Instructor: Jed S Rakoff			

	AHRS	EHRS
Current	16.0	16.0
Cumulative	46.0	46.0

Spring 2023

School of Law
Juris Doctor
Major: Law

Complex Litigation	LAW-LW 10058	4.0	A-
Instructor: Samuel Issacharoff, Arthur R Miller			
Intelligence: Law, Strategy, Ethics Seminar	LAW-LW 10439	2.0	A
Instructor: Samuel J Rascoff			
Evidence	LAW-LW 11607	4.0	A
Instructor: Daniel J Capra			
Strategic Human Rights Litigation Seminar	LAW-LW 12531	2.0	A
Instructor: Philip G Alston, James Andrew Goldston			

	AHRS	EHRS
Current	12.0	12.0
Cumulative	58.0	58.0

Butler Scholar - Top Ten Students in the Class after four semesters
Staff Editor - Law Review 2022-2023

End of School of Law Record

TRANSCRIPT ADDENDUM FOR NYU SCHOOL OF LAW
JD CLASS OF 2023 AND LATER & LLM STUDENTS

I certify that this is a true and accurate representation of my NYU School of Law transcript.

Grading Guidelines

Grading guidelines for JD and LLM students were adopted by the faculty effective fall 2008. These guidelines represented the faculty's collective judgment that ordinarily the distribution of grades in any course will be within the limits suggested. An A + grade was also added.

Effective fall 2020, the first-year J.D. grading curve has been amended to remove the previous requirement of a mandatory percentage of B minus grades. B minus grades are now permitted in the J.D. first year at 0-8% but are no longer required. This change in the grading curve was proposed by the SBA and then endorsed by the Executive Committee and adopted by the faculty. Grades for JD and LLM students in upper-level courses continue to be governed by a discretionary curve in which B minus grades are permitted at 4-11% (target 7-8%).

First-Year JD (Mandatory)	**All other JD and LLM (Non-Mandatory)**
A+: 0-2% (target = 1%) (see note 1 below)	A+: 0-2% (target = 1%) (see note 1 below)
A: 7-13% (target = 10%)	A: 7-13% (target = 10%)
A-: 16-24% (target = 20%)	A-: 16-24% (target = 20%)
Maximum for A tier = 31%	***Maximum for A tier = 31%***
B+: 22-30% (target = 26%)	B+: 22-30% (target = 26%)
Maximum grades above B = 57%	***Maximum grades above B = 57%***
B: remainder	B: remainder
B-: 0-8%*	B-: 4-11% (target = 7-8%)
C/D/F: 0-5%	C/D/F: 0-5%

The guidelines for first-year JD courses are mandatory and binding on faculty members; again noting that a mandatory percentage of B minus grades are no longer required. In addition, the guidelines with respect to the A+ grade are mandatory in all courses. In all other cases, the guidelines are only advisory.

With the exception of the A+ rules, the guidelines do not apply at all to seminar courses, defined for this purpose to mean any course in which there are fewer than 28 students.

In classes in which credit/fail grades are permitted, these percentages should be calculated only using students taking the course for a letter grade. If there are fewer than 28 students taking the course for a letter grade, the guidelines do not apply.

Important Notes

1. The cap on the A+ grade is mandatory for all courses. However, at least one A+ can be awarded in any course. These rules apply even in courses, such as seminars, where fewer than 28 students are enrolled.
2. The percentages above are based on the number of individual grades given – not a raw percentage of the total number of students in the class.
3. Normal statistical rounding rules apply for all purposes, so that percentages will be rounded up if they are above .5, and down if they are .5 or below. This means that, for example, in a typical first-year class of 89 students, 2 A+ grades could be awarded.
4. As of fall 2020, there is no mandatory percentage of B minus grades for first-year classes.

NYU School of Law does not rank students and does not maintain records of cumulative averages for its students. For the specific purpose of awarding scholastic honors, however, unofficial cumulative averages are calculated by the Office of Records and Registration. The Office is specifically precluded by faculty rule from publishing averages and no record will appear upon any transcript issued. The Office of Records and Registration may not verify the results of a student's endeavor to define his or her own cumulative average or class rank to prospective employers.

Scholastic honors for JD candidates are as follows:

Pomeroy Scholar:	Top ten students in the class after two semesters
Butler Scholar:	Top ten students in the class after four semesters
Florence Allen Scholar:	Top 10% of the class after four semesters
Robert McKay Scholar:	Top 25% of the class after four semesters

Named scholar designations are not available to JD students who transferred to NYU School of Law in their second year, nor to LLM students.

Missing Grades

A transcript may be missing one or more grades for a variety of reasons, including: (1) the transcript was printed prior to a grade-submission deadline; (2) the student has made prior arrangements with the faculty member to submit work later than the end of the semester in which the course is given; and (3) late submission of a grade. Please note that an In Progress (IP) grade may denote the fact that the student is completing a long-term research project in conjunction with this class. NYU School of Law requires students to complete a Substantial Writing paper for the JD degree. Many students, under the supervision of their faculty member, spend more than one semester working on the paper. For students who have received permission to work on the paper beyond the semester in which the registration occurs, a grade of IP is noted to reflect that the paper is in progress. Employers desiring more information about a missing grade may contact the Office of Records & Registration (212-998-6040).

Class Profile

The admissions process is highly selective and seeks to enroll candidates of exceptional ability. The Committees on JD and Graduate Admissions make decisions after considering all the information in an application. There are no combination of grades and scores that assure admission or denial. For the JD Class entering in Fall 2021 (the most recent entering class), the 75th/25th percentiles for LSAT and GPA were 174/170 and 3.93/3.73.

Updated: 10/4/2021

New York University
A private university in the public service

School of Law

40 Washington Square South
New York, New York 10012-1099
Telephone: (212) 998-6160
Facsimile: (212) 995-4894
Email: liam.murphy@nyu.edu

Liam Murphy
Herbert Peterfreund Professor of Law
& Professor of Philosophy

June 5, 2023

Dear Judge

It is a pleasure to write in support of JOSHUA ZAKHAROV's application for a clerkship in your chambers. Josh was a stand-out student in my contracts class last year. On the basis of his classroom performance and his excellent exam, I asked him to be one of my TAs this past fall. I know him very well.

Josh is already a very impressive young lawyer. His performance in law school puts him at the very top of his class. He is a Pomeroy Scholar—one of the ten best performing students in the first year—and his second-year performance maintained that level of all-around excellence. In my contracts class, he was a frequent and cheerful volunteer, one of the students I could count on to end a moment of silence. His choice of courses—from a judicial externship in the E.D.N.Y. to a seminar in comparative constitutional law, from complex litigation to a seminar on strategic human rights litigation—show a remarkable breadth and depth of interest. That he excels in all these domains, from the most theoretical to the most legal-practical, augers well, I believe, for his value as a clerk.

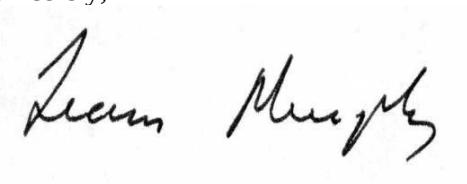
But it is perhaps the Josh I know from working with him as a TA that is most relevant to his special qualifications for a clerkship. My practice is to ask my TAs to discuss sample problems with a section of the contracts class. Every other week, I meet with the TAs as a group to discuss the sample problems—which they take turns drafting. These sessions, where the TAs essentially workshop each other's problems are very enjoyable for me as a teacher as I get to observe a group of very talented students engage collaboratively with one another. I have always thought that students who perform exceptionally well in this context are excellent candidates for clerkships—Josh is such a case. Not only did Josh come with excellent drafts of his own, but he was also incredibly quick at picking up on worries that others had, nailing down the worry, and fixing the problem with dispatch. So he clearly can take constructive critical feedback very well.

Perhaps even more valuable, since his own drafts rarely needed much improvement, was his ability to suggest improvements to others' work. Josh exudes kindness and helpfulness, so much so that what is, in fact, the identification of a serious problem might be received as a kind of encouraging compliment with a suggestion about how to make things even better. It was quite wonderful to see this combination of kindness and brilliance at work in a collaborative context.

Josh has a great future ahead of him, one that will much benefit his country. I have mentioned the breadth of Josh's interests. But this is not dilettantism on his part. Rather, he aims for a career that can combine his core interests in international, private, and comparative law. He has already identified relevant programs in different departments of the Federal Government that allow for his. I have not the slightest doubt that important and original legal work will be done by Josh in the future.

Josh is very intelligent, very hard-working, an excellent writer, and an excellent lawyer with an already impressively diverse range of expertise. He is also, as I have emphasized, an extremely effective collaborator and a kind, lovely person. I recommend him very warmly and in the highest terms. Please do feel free to contact me if I may be of any further assistance.

Sincerely,



June 13, 2023

The Honorable Kenneth Karas
Charles L. Brieant, Jr. United States Courthouse
300 Quarropas Street, Room 533
White Plains, NY 10601-4150

Dear Judge Karas:

Joshua Zakharov, a candidate for the JD in the class of 2024, has asked me to write on his behalf in connection with his applications for judicial clerkship. I am delighted to have this opportunity to write on his behalf as Mr. Zakharov, the son of Soviet emigres, is truly one of the most gifted students that I have had an opportunity to teach in my dozen years at New York University's School of Law. He has my highest recommendation.

It is rare for me to award students with an A+ in any of my classes as this is a grade that professors are not required to give under NYU's strict first year grading curve. Like many of my colleagues on the faculty, I reserve that grade to students whose exam preference is at least ten points above the next best student received. It has been some years since I last awarded that grade in my first year international law course (one of eight electives offered to our one-Ls). Mr. Zakharov exceeded my internal standards and was far and away the best exam in that course – and among the best that I have ever seen in teaching that course for nearly 30 years. (I also note that he was one of the few students that I have seen to have secured the same A+ grade twice in his first year.) International law – which is actually more of a curriculum than a single course insofar as its subject matter essentially addresses all first year subjects (from contracts to civil procedure) whenever these topics involve the crossing of an international border – is probably the most difficult of our first year elective courses. Mr. Zakharov – an active participant from the first day of the course – wrote an astonishingly comprehensive and well- written response to an exam that required the ability to answer detailed factual hypotheticals, jurisprudential inquiries, and mastery over black-letter doctrine.

As is evident from his transcript, Mr. Zakharov's performance in my class was replicated throughout his first year at the law school. Mr. Zakharov's transition from magna cum laude graduate of the University of Chicago to NYU law school has been seamless. As is clear from his achieving Pomeroy Scholar status, Mr. Zakharov is at the top of his class, with all of his first year grades in the A range. Clearly our admissions office was not wrong to attract him from rival law schools with a merit-based scholarship. He is one of the few students that I have encountered that I can truly say was born to be a lawyer – and not only because he clearly has thrived on the Law Review as he did in competitive debate prior to applying to law school. His talents have been evident among all of us teaching first year students. It appears that many of us competed to have him serve as a teaching assistant (TA) in our first year courses as he entered his second law school year. Indeed, I was too late in that competition as my colleague, Prof. Murphy managed to entice him to serve as her TA in first year contracts (while another colleague, Sam Issacharoff managed to snatch him as a research assistant). Mr. Zakharov served as my TA in the international law first year elective purely on his own time. Astonishingly, he volunteered to do this without receiving the usual TA academic credit and on top of a full load of courses, considerable responsibilities as a TA for another course, and deep commitments for the law review. He did an exceptional job as my TA. Over the past 13 weeks he became a highly trustworthy assistant who has earned praise from the many first year students who regularly came to his weekly office hours and those who participated in seven 'optional' working sessions that he has helped to organize and teach. Mr. Zakharov is obviously adept at not only absorbing new knowledge quickly but also in conveying that knowledge to others. Assuming he succeeds in his applications for a judicial clerkship, I would expect him to be part of a collegial team capable of imparting lessons learned within the group.

Despite his limited time in law school, Mr. Zakharov has had an unusually diverse set of experiences in the law. Very second year law students have, as he has, worked in the chambers of a US district judge, been exposed to international financial disputes and arbitration, deployed quantitative skills to address trade policy, or used foreign language skills to advance the goals of the U.S. State Department in Uzbekistan. Given his diverse talents and interests in the law, I am not surprised that he is considering both trial and appellate clerkships as well as other public interest and private law firms in the immediate short term. He would excel in any of these capacities – and indeed would make a terrific academic should he decide to go in that direction. (He is under consideration to become a Furman fellow here – an honor we reserve to those whom the faculty identifies as having the talent and aptitude to become law professors.)

It is also important to point out that Mr. Zakharov is more than his sterling GPA suggests. Mr. Zakharov is engaging, has a sense of humor, works well with others, and, despite his accomplishments, is unassuming and a pleasure to work with. He has managed to educate me about what it means to genuinely listen and care for others.

There is no question in my mind that he would be an asset to any chambers lucky enough to have him.

Sincerely yours,
José E. Alvarez
Herbert and Rose Rubin Professor of International Law

Jose Alvarez - jose.alvarez@nyu.edu - (212) 992-8835

New York University
A private university in the public service

School of Law
Faculty of Law

40 Washington Square South
New York, NY 10012-1099
Telephone: (212) 998-6580
Facsimile: (212) 995-4590
E-mail: samuel.issacharoff@nyu.edu

Samuel Issacharoff
Reiss Professor of Constitutional Law

Dear Judge:

I have been teaching for over 30 years and have taught thousands of students and worked closely with hundreds as teaching or research assistants, or in supervision of independent research. To recommend Josh Zakharov for a clerkship, I have to reach back to the comparisons with the handful that stand out as truly superlative. He is a dazzling intellect, so full of vibrancy and inquiry, so eager to learn and engage ideas, so thoughtful. He is a star by any measure.

The easy part of the recommendation is the formal credentials. He is one of the top ten students in the class. He is on law review. He has all A-level grades – indeed he would have a 4.0 GPA had he not ended up one point short of the A/A- divide in my complex litigation class. He has a wonderful undergraduate education from the University of Chicago, the school that year in, year out provides many of my best students. Something in the air in Hyde Park seems to prompt great critical inquiry and a joy in learning, and Josh is certainly an exemplar of both.

Josh was a student of mine his first semester of law school. He immediately impressed me with the precision of his comments and questions. He was not overly assertive initially, but I took note that every time he spoke the discussion advanced substantially. I also took note of his writing. In first semester civil procedure, I give three graded writing assignments, and Josh was clearly a gifted writer, evident in even the short essays. He then ended up with the highest grade in my class.

I hired Josh to work for me as an RA over his first summer, on an overload basis. He was working in the Hague and then in Kyrgyzstan, and used his extra time to produce extraordinary work as I was finishing my book on Democracy Unmoored. Even here, Josh was much more engaging than simply great research work. He is a truly fascinating person with far-ranging interests. He came to law school with interests in international affairs, national security, and Central Asia. He scoured databases on foreign law firms that would hire an American intern, and ended up spending 6 weeks in Bishkek, the capital of Kyrgyzstan, at a commercial firm that needed help on some international arbitration matters. He is headed neither to practice in Central Asia nor most likely to commercial arbitration. But he wanted to encounter what the legal world looked like in a legally-unsettled former Soviet Republic. I recall having zoom sessions with him from this home in Bishkek, certainly one of the more unusual research meetings I have had.

Josh continued to work for me as a research assistant in his second year, until law review and other tasks started to consume his time. I also had regular dealings with him in my Complex Litigation course, where he engaged the materials at a level that just stood out. But for one silly mistake on the exam, he would have easily had an A, perhaps an A+. He is just stellar at everything he touches, and he is also a delightful person to work with. His interests now gravitate toward national security and comparative constitutional law and complex litigation. While life will force him to sort that out, these areas dovetail with

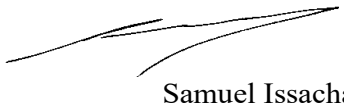
critical interests of mine, allowing for a great deal of fruitful exchange, even beyond the work requirements of class or being a research assistant. In fact, I value not only his smarts but his judgment, and look forward to my exchanges with him as I would with a junior colleague.

After taking Complex Litigation, Josh decided to write his student note on one of the more difficult problems in aggregate litigation today: the extent of closure that can be realized through different joinder mechanisms. Specifically, he is looking at two recent decisions from the Third and Seventh Circuit on efforts to use issue preclusion through pretrial orders in MDLs and at a very recent Tenth Circuit decision on the expanded use of issue classes. I am supervising his Note and have seen the initial drafts dealing with *Home Depot* and *Looper*, the two issue preclusion cases. It is thoughtful, engaging, and well-crafted, just as I would have expected.

Josh has already accepted a clerkship with Judge Anthony Scirica beginning when he graduates in 2024. I have over the years recommended a number of my star students to Judge Scirica, and had no hesitation in recommending Josh to him. Josh is now looking for a district court clerkship after he finishes with Judge Scirica. As should be evident, I think Josh is a genuine star and will make a great law clerk. I have only the best things to say about him.

Please feel free to call if there is any further information I can provide.

Sincerely,



Samuel Issacharoff

Writing Sample

This writing sample is a draft order on a motion to dismiss a False Claims Act complaint, which I wrote as an extern to Judge Kovner in the fall semester of 2022. It was released to me from chambers and approved with redactions of party names, the caption and case number, and other identifying information. I am the sole author with the exception of the paragraph stating the standard of review for 12(b)(6) motions, which is common across drafts in chambers. I have also edited it for length.

In 2015, plaintiff [redacted] brought this *qui tam* action against defendants [redacted] and [redacted], alleging fraud and retaliation in violation of 31 U.S.C. §§ 3729(a)(1)(A-B), 3729(a)(2), and 3730(h) ("FCA") and N.Y. State Fin. Law §§ 189(1)(a-b) and 191 ("NYFCA"). Defendants moved to dismiss the complaint for failure to state a claim. For the reasons discussed below, plaintiff's FCA and NYFCA fraud claims are dismissed, but his retaliation claims may proceed.

BACKGROUND

The following is a summary of the allegations contained in plaintiff's complaint. From 2007 to 2014 plaintiff was employed by [redacted] ("[redacted]"), a New York provider of medical transportation and ambulance services led by Chief Executive Officer [redacted]. Compl. ¶ 16 (Dkt. #22). Plaintiff worked first as a [redacted], then as [redacted] and [redacted], and then again as a [redacted] after a demotion. *Id.* ¶ 12. [redacted] terminated plaintiff's employment in July 2014. *Id.* ¶ 87. [redacted] receives "millions of dollars a year" in reimbursements from Medicare and New York Medicaid for providing services to patients covered by those programs. *Id.* ¶ 19.

Plaintiff alleges that during his tenure, [redacted] engaged in a two-part fraudulent scheme to make false claims for reimbursement from government programs. First, [redacted] impermissibly provided ambulance and medical transportation services outside of its "primary territory" in violation of New York Medicaid and Medicare coverage rules. *Id.* ¶¶ 104, 31. Plaintiff references several hospitals outside of [redacted]'s primary territory to which [redacted] provided services, a subcontract with another EMS service whose patients [redacted] would serve outside of [redacted]'s primary territory, and dates on which the services were provided. *Id.* ¶ 42. To avoid detection, [redacted] would then knowingly falsify Prehospital

Care Reports ("PCRs"), inserting inaccurate location codes to make it appear as though services [redacted] provided outside its primary territory were provided within it. *Id.* ¶¶ 48, 52.

Second, [redacted] provided ambulance services that were "not medically necessary . . . regardless of whether the patients' medical conditions require[d] ambulance transport, or, alternatively, would have permitted the patient to use a . . . less expensive form of transport," including transport for patients who were "ambulating normally" and "feeling fine." *Id.* ¶ 54. Then, on [redacted]'s instruction, [redacted] would "include false information about patients' conditions on the PCRs" to mask this scheme as well. *Id.* ¶¶ 61–62. Based on these false PCRs, [redacted] would then submit false claims to Medicare using the CMS-1500 form, and to New York Medicaid using the New York State eMedNY-000201 claim form. *Id.* ¶¶ 67, 73.

Plaintiff further alleges that after raising concerns about these fraudulent practices to [redacted] and other agents of [redacted], [redacted] retaliated against him with verbal harassment, *id*. ¶ 80, demotion, *id*. ¶ 85, and eventually termination, *id*. ¶ 87. For example, in May 2012, after plaintiff received an assignment that he believed would violate the primary territory rules, he notified his dispatcher. *Id.* ¶ 80. The dispatcher responded by instructing him to "do the . . . call," and another [redacted] agent contacted plaintiff the following day and told him to "keep quiet and mind [his] business." *Ibid.* That same year, plaintiff approached [redacted] "with his concern that the company was breaking the rules" as to primary territory operations, *id.* ¶ 79, to which [redacted] responded by telling plaintiff not to pursue those concerns further. *Ibid.* Two years later, after plaintiff told [redacted] that "he would not go along with breaking the law" by "changing codes" on PCRs, [redacted] demoted plaintiff from his operations position to "the lowest level [redacted]," stopped automatic deductions from plaintiff's paycheck for child support, "ultimately laid

[plaintiff] off," distributed memoranda around [redacted] disparaging plaintiff, and sued plaintiff. *Id.* ¶¶ 85-89.

Plaintiff filed this action in 2015 asserting four *qui tam* claims, two under the False Claims Act (FCA) and two under the New York False Claims Act (NYFCA), and two whistleblower retaliation claims, one under the FCA and one under the NYFCA.

New York State declined to intervene on November 12, 2021, and the federal government declined to intervene on November 17, 2021. The State of New York's Notice of Election to Decline Intervention (Dkt. #16); The Government's Notice of Election to Decline Intervention (Dkt. #17). Following the government's declinations to intervene, plaintiff's counsel moved to withdraw as counsel on February 1, 2021, which the Court granted but stayed the withdrawal until March 2, 2022 so that plaintiff had time to find new representation. Order dated February 16, 2022. Instead, plaintiff opted to proceed *pro se* and refiled his complaint shortly thereafter. Notice of Req. to Continue Pro Se (Dkt. #21); Notice of False Claims Act Compl. (Dkt. #22).

Defendants moved to dismiss, and plaintiff did not reply by the original, first-extended, or second-extended deadline, Order dated June 23, 2022, and the Court "consider[s] defendants' motion fully briefed." Order dated August 25, 2022; *Kinnion v. Comm'r of Soc. Sec.*, No. 17-CV-06455 (AMD), 2019 WL 982508, at *1 (E.D.N.Y. Feb. 27, 2019).

STANDARD OF REVIEW

To survive a Federal Rule of Civil Procedure 12(b)(6) motion to dismiss, a complaint must contain "enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). A claim is plausible "when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). A complaint fails

to plausibly state a claim and is properly dismissed when "the allegations in a complaint, however true, could not raise a claim of entitlement to relief" as a matter of law, *Twombly*, 550 U.S. at 558, or when "the well-pleaded facts do not permit the court to infer more than the mere possibility of misconduct" as matter of law, *Iqbal*, 556 U.S. at 679.

DISCUSSION

Pro se plaintiff's *qui tam* FCA and NYFCA fraud claims are dismissed because neither can be brought by a *pro se* litigant, and plaintiff is not represented by counsel. But he sufficiently alleges his FCA and NYFCA retaliation claims and they may proceed.

I. Plaintiff's *qui tam* FCA and NYFCA fraud claims are dismissed.

Plaintiff attempts to proceed *pro se* in a *qui tam* capacity on his federal and state FCA claims. Compl. ¶ 1 (Dkt. #22). "The FCA permits private persons to bring suit where there has been fraud on the federal government. The *qui tam* provisions of the FCA allow a private plaintiff to sue persons who knowingly defraud the federal government." *Kelly v. New York*, No. 19-CV-2063 (JMA) (ARL), 2020 WL 7042764, at *11 (E.D.N.Y. Nov. 30, 2020) (quoting *United States ex rel. Honda v. Passos*, No. 20-CV-3977, 2020 WL 3268350, at *2 (S.D.N.Y. June 15, 2020)). "However, *pro se* litigants lack standing to bring *qui tam* claims under the FCA." *Kelly*, 2020 WL 7042764, at *11 (citing *United States ex rel. Mergent Servs. v. Flaherty*, 540 F.3d 89, 93 (2d Cir. 2008)).

Pro se litigants lack standing to bring *qui tam* claims because when a party files a *qui tam* claim under the False Claims Act or a state equivalent, they are "not litigating his or her own interest, but rather, the interest of the government." *Bowens v. Corr. Ass'n of New York*, No. 19-CV-1523 (PKC) (CLP), 2019 WL 1586857, at *5 (E.D.N.Y. Apr. 12, 2019) (quoting *United States ex rel. Mergent Servs.*, 540 F.3d at 93). Another's interest cannot be litigated *pro se*, since "only

one licensed to practice law may conduct proceedings in court for anyone other than himself." *United States v. Onan*, 190 F.2d 1, 6 (8th Cir. 1951). Because plaintiff is alleging fraud claims against not him but the United States and New York State, he is therefore "not litigating his . . . own interest" and cannot effectively represent the United States—the nature of a *qui tam* suit—*pro se*. *Bowens*, 2019 WL 1586857, at *5. Thus, those claims must be dismissed. In *Kelly*, for example, the court dismissed plaintiff's FCA claims "[b]ecause Plaintiff, a non-lawyer *pro se* litigant, lack[ed] standing," so "his FCA claims [were] not plausible." *Kelly*, 2020 WL 7042764, at *11; *see also United States ex rel. Mergent Servs.*, 540 F.3d at 93 (noting that because relators "lack a personal interest" in *qui tam* actions, they are not the real party in interest and "the right to bring the claim belongs to the United States," not to relators to assert *pro se*); *Palmer v. Fannie Mae*, 14-CV-4083 (JFB)(AYS), 2016 WL 5338542, at *4 (E.D.N.Y. Sept. 23, 2016) ("The law in this Circuit is clear that *pro se* litigants may not pursue *qui tam* actions under the False Claims Act."). This case is no different.

The same is true of claims brought under the New York False Claims Act. Federal law informs the interpretation of the NYFCA in general as "New York courts look toward federal law when interpreting the New York [False Claims] [A]ct," so it is instructive that federal law does not allow *qui tam* suits to proceed *pro se*. *State ex rel. Seiden v. Utica First Ins.*, 943 N.Y.S. 2d 6, 39 (App. Div. 2012). Furthermore, New York State regulations pertinent to the New York False Claims Act reflect federal law's rejection of *pro se* FCA *qui tam* suits by non-attorneys. N.Y. Proc. Regs. of False Claims Act § 400.4(d) ("If the state or a local government decides not to intervene or supersede in a qui tam action, the *qui tam* plaintiff may not pursue the *qui tam* action on a *pro se* basis unless the *qui tam* plaintiff is an attorney."); *see State ex rel. Banerjee v. Moody's Corp.*,

42 N.Y.S. 627, 629 (N.Y. Sup. Ct. 2016) (describing § 400.4 as "applicable law[]" in a New York False Claims Act case).

Plaintiff's FCA and NYFCA *qui tam* claims therefore must be dismissed because they may not be brought *pro se*.

II. Plaintiff's FCA and NYFCA retaliation claims may proceed.

Because plaintiff sufficiently alleges that he was harassed, demoted, and terminated because of his attempt to remedy his employer's alleged FCA and NYFCA violations, his retaliation claims may proceed. Compl. ¶¶ 109-112 (Dkt. #22).

While a plaintiff may not proceed *pro se* on fraud claims under the False Claims Act, a plaintiff *may* proceed *pro se* on retaliation claims under the False Claims Act. Courts in this Circuit have regularly allowed FCA retaliation claims to proceed *pro se* because the real party in interest in retaliation claims, unlike in *qui tam* claims, is the *pro se* plaintiff. *See Hayes v. Dept. Of Educ. of City of New York*, 20 F. Supp. 3d 438, 443 (S.D.N.Y. 2014) (collecting cases); *Weslowski v. Zugibe*, 14 F. Supp. 3d 295, 309-10 (S.D.N.Y. 2014) (explaining that a *pro se* "FCA retaliation claim is materially different . . . from a relator-initiated FCA claim . . . whereas a relator-initiated FCA claim is a claim brought on behalf of the United States, an FCA retaliation claim is a personal or private cause of action brought on behalf of the individual"). Furthermore, the dismissal of plaintiff's fraud claims does not necessarily imperil his FCA and NYFCA retaliation claims. *See United States v. N. Adult Daily Health Care Ctr.*, 205 F. Supp. 3d 276, 298 (E.D.N.Y. 2016) ("[A] plaintiff need not prevail on his underlying FCA claims" to state a claim of retaliation, "but he must demonstrate that he had been investigating matters that were calculated, or reasonably could have [led], to a viable FCA claim.") (internal quotations omitted).

To state a claim of retaliation under the FCA, plaintiff must allege "(1) that he engaged in activity protected under the statute; (2) that the employer was aware of such activity; and (3) that the employer took adverse action against him because he engaged in the protected activity." *Dhaliwal v. Salix Pharm., Ltd.*, 752 F. App'x 99, 100 (2d. Cir. 2019) (quoting *United States ex rel. Chorches for Bankr. Est. of Fabula v. Am. Med. Response, Inc.*, 865 F.3d 71, 95 (2d Cir. 2017)). Activity protected under the FCA refers to "lawful acts done by the employee . . . in furtherance of an [FCA] action . . . or other efforts to stop 1 or more [FCA] violations." 31 U.S.C.A. § 3730(h)(1). This includes "refusal to engage in a fraudulent scheme, which under the facts as pled was intended and reasonably could be expected to prevent the submission of a false claim to the government." *United States ex rel. Chorches*, 865 F.3d at 96. An adverse action under the FCA includes termination or loss of employment, *id.* at 93, demotion, *Garcia v. Aspira of New York, Inc.*, No. 07 Civ. 5600(PKC), 2011 WL 1458155, at *3 (S.D.N.Y. Apr. 13, 2011), harassment, and "any other form of retaliation," *Faldetta v. Lockheed Martin Corp.*, No. 98 Civ. 2614(RCC), 2000 WL 1682759, at *11 (S.D.N.Y. Nov. 9, 2000). *See* 31 U.S.C.A. § 3730(h). Although it does apply to fraud claims under the FCA, "Rule 9(b)'s heightened pleading standard does not apply to . . . FCA retaliation claim[s] since no showing of fraud is required," so plaintiff's claims of retaliation need only be plausible to proceed. *United States ex rel. Mooney v. Americare, Inc.*, No. 06–CV–1806 (FB)(VVP), 2013 WL 1346022, at *8 (E.D.N.Y. Apr. 3, 2013); *see Twombly*, 550 U.S. at 570; *Iqbal*, 556 U.S. at 678.

Plaintiff's complaint plausibly alleges all three elements. First, plaintiff claims he engaged in protected activity under the FCA and NYFCA. Once "he learned about the primary territory restrictions and realized that [redacted] was operating in violation of them," he "approached [redacted] with his concern that [[redacted]] was breaking the rules" and refused to

"go along with breaking the law." Compl. ¶¶ 79, 85 (Dkt. #22). Both declining to perform services that plaintiff reasonably believed violated the FCA and approaching [redacted] with concerns about those services constitute protected activity under the FCA. *United States ex rel. Chorches*, 865 F.3d at 96 (holding that refusal to falsify a PCR, exactly the report plaintiff alleges [redacted] was falsifying, is protected activity under the FCA); *Dhaliwal*, 752 F. App'x at 101 (finding that "raising a concern that [plaintiff's employer] was potentially committing 1 or more violations of the FCA" is protected activity) (internal quotations omitted).

Second, plaintiff alleges his employer's awareness of his protected activity. Plaintiff alleges not only that [redacted] and [redacted] were aware of his refusal to go along with the scheme, but also that they urged plaintiff not to pursue his concerns with the scheme any further. Compl. ¶¶ 79-80 (Dkt. #22); *id.* ¶ 85. For example, when plaintiff informed [redacted] circa May 2012 of his suspicion that [redacted] was submitting false claims, a [redacted] agent told plaintiff to "keep quiet" and to "mind [his] business." *Ibid.* Plaintiff continued conveying his concerns and refusal to participate in PCR falsification to [redacted] agents and [redacted] regularly from May 2012 through April 2014. *Id.* ¶¶ 79-84.

Finally, plaintiff alleges that his employer took adverse action against him because of that protected activity. Defendants "demoted [plaintiff]" from his [redacted] position to a low-level [redacted] "in response to [plaintiff's] raising concerns about out-of-territory ambulance services" and stopped automatic child support deductions from his pay without his consent, causing default. *Id.* ¶¶ 84-86. Plaintiff also alleges that the retaliation continued beyond his departure from [redacted], including with a retaliatory lawsuit and the distribution of a "memo" at [redacted] stating that "[a]nyone that can catch [plaintiff] working . . . with [other ambulance services] . . . will receive a finder's fee." *Id.* ¶ 88. These allegations, asserting that

plaintiff was harassed, demoted, and eventually terminated as a result of his complaints of fraud to [redacted], are thus sufficient to state a claim for retaliation. *See N. Adult Daily Health Care Ctr.*, 205 F. Supp. 3d at 300 (E.D.N.Y. 2016) (finding allegations of demotion and termination because of protected conduct to be sufficient to state a claim under the FCA and NYFCA).

Plaintiff also alleges violations of § 191 of the NYFCA for the same conduct. Finding a violation of the federal False Claims Act's provisions against retaliation would entail finding a violation of the analogous state provisions. When a plaintiff sufficiently states an FCA retaliation claim, they also sufficiently state an NYFCA retaliation claim. *Krause v. Eihab Human Servs.*, No. 10 CV 898 (RJD) (SMG), 2015 WL 4645210, at *4 (E.D.N.Y. Aug. 4, 2015) ("The whistleblower provision of the New York FCA [§ 191] is essentially identical in language and substance to its federal counterpart." (quoting *Forkell v. Lott Assisted Living Corp.*, No. 10–CV–5765 (NRB), 2012 WL 1901199, at *13 (S.D.N.Y. May 21, 2012))); *id.* at *6 (applying the same analysis to find both FCA and NYFCA retaliation claims). The foregoing thus applies with equal force to plaintiff's state law retaliation claims.

Thus, by alleging that he engaged in a protected activity of which his employer was aware and on the basis of which his employer took an adverse action against him, plaintiff sufficiently states his FCA and NYFCA retaliation claims. Those claims may proceed notwithstanding the failure of plaintiff's fraud claims.

CONCLUSION

Defendants' motion to dismiss is granted as to plaintiff's FCA and NYFCA fraud claims. Defendants' motion to dismiss is denied as to plaintiff's FCA and NYFCA retaliation claims.